

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOCUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

PROCEDURA OPERATIVA GENERALE

“MANUALE DI GESTIONE DOCUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”

Emesso/Redatto	Verificato da	Controllo formale	Approvato
Coordinatore Gruppo di lavoro	Dirigente struttura/Direttore Dipartimento*	SC Qualità e Sicurezza delle Cure	☐ Comitato di Direzione ☒ Direttore Generale ☐ Direttore di Dipartimento
<i>Firmato digitalmente*</i>		<i>Firmato digitalmente*</i>	<i>Firmato digitalmente*</i>
Firmato da: CLARA PELLICIA Valido da: 19-06-2024 15:48:11 a: 19-06-2027 02:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale "SigningTime": 25-06-2025 15:30:46 Motivo: Approvo il documento		Firmato da: ROBERTO GENCO RUSSO Valido da: 12-11-2024 13:40:44 a: 12-11-2027 02:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale "SigningTime": 18-06-2025 17:12:29 Motivo: Approvo il documento	Firmato da: PAOLA PALMIERI Valido da: 15-09-2022 12:31:51 a: 15-09-2025 02:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale "SigningTime": 04-07-2025 12:28:23 Motivo: Approvo il documento

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

SOMMARIO

1. DISPOSIZIONI GENERALI	5
1.1 Elenco revisioni	5
1.2 Gruppo di lavoro	6
1.3 Premessa	6
1.4 Ambito di applicazione.....	8
1.5 Definizioni generali	8
1.6 Acronimi	11
2. ARTICOLAZIONE E ORGANIZZAZIONE DELLE STRUTTURE	12
2.1 Area Organizzativa Omogenea.....	12
2.2 Responsabilità della gestione dei flussi documentali e degli archivi.....	12
2.3 Articolazione dell’Agenzia.....	13
2.4 Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.....	13
2.5 Unicità del protocollo informatico	15
2.6 Modello operativo adottato per la gestione dei documenti	15
3. FORMAZIONE DEI DOCUMENTI	15
3.1 Modalità di formazione dei documenti e contenuti minimi	15
3.2 Formato dei documenti informatici.....	16
3.3 Sottoscrizione dei documenti informatici.....	16
3.4 Valore probatorio del documento informatico.....	17
3.5 Documenti cartacei: originali, minute e copie.....	17
3.6 Documenti informatici: originali, duplicati e copie.....	18
3.7 Tutela della riservatezza.....	18
4. RICEZIONE DEI DOCUMENTI	18
4.1 Ricezione dei documenti su supporto cartaceo.....	18
4.2 Ricezione dei documenti informatici	19
4.3 Ricevute attestanti la ricezione dei documenti	20
4.4 Conservazione delle buste o altri contenitori di documentazione	20
4.5 Orari di apertura per il ricevimento della documentazione cartacea.....	20
5.REGISTRAZIONE DEI DOCUMENTI	20

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

5.1 Documenti ricevuti, spediti, interni	20
5.2 Documenti soggetti a registrazione di protocollo.....	21
5.3 Documenti non soggetti a registrazione obbligatoria di protocollo.....	21
5.4 Registrazione di protocollo dei documenti	22
5.5 Segnatura di protocollo.....	23
5.6 Annullamento delle registrazioni di protocollo	23
5.7 Differimento dei termini di registrazione.....	24
5.8 Registro giornaliero e annuale di protocollo	24
5.9 Registro di emergenza	24
6. CASI PARTICOLARI.....	24
6.1 Documentazione soggetta a registrazione particolare	24
6.2 Documentazione di gare d'appalto	25
6.3 Documenti a carattere riservato, personale e /o confidenziale	25
6.4 Lettere anonime	25
6.5 Documenti con firma illeggibile	25
6.6 Documenti non firmati.....	26
6.7 Corrispondenza con più destinatari	26
6.8 Allegati	26
6.9 Documentazione di competenza di altre amministrazioni o di altri soggetti	26
6.10 Documenti originali plurimi o in copia per conoscenza.....	26
6.11 Oggetti plurimi	26
6.12 Produzione seriale di documenti sulla base di un modello generale	27
6.13 Modelli pubblicati	27
6.14 Trasmissioni telematiche	27
6.15 Documentazione gestionale interna.....	28
7. GESTIONE DELLA POSTA ELETTRONICA	28
7.1 La posta elettronica nelle comunicazioni interne all'Agenzia.....	29
7.2 La posta elettronica nelle comunicazioni verso l'esterno (Pubbliche Amministrazioni, cittadini e altri soggetti privati)	29
7.3 La posta elettronica ricevuta da cittadini o altri soggetti privati.....	30
7.4 La posta elettronica ricevuta da altre Pubbliche Amministrazioni.....	31
8. ASSEGNAZIONE E CLASSIFICAZIONE DEI DOCUMENTI.....	31

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

8.1 Assegnazione.....	31
8.2 Modifica delle assegnazioni.....	31
8.3 Consegna dei documenti cartacei.....	32
8.4 Consegna dei documenti informatici.....	32
8.5 Classificazione dei documenti	32
9. FASCICOLAZIONE DEI DOCUMENTI.....	32
9.1 Formazione e identificazione dei fascicoli.....	32
9.2 Processo di formazione dei fascicoli.....	33
9.3 Modifica delle assegnazioni dei fascicoli.....	34
9.4 Tenuta dei fascicoli dell'Archivio corrente	34
9.5 Scambio di documenti o di fascicoli fra gli uffici dell'Agenzia	34
10. SPEDIZIONE DEI DOCUMENTI DESTINATI ALL'ESTERNO	34
10.1 Spedizione dei documenti cartacei	34
10.2 Spedizione dei documenti informatici.....	35
11. SCANSIONE DEI DOCUMENTI CARTACEI.....	36
11.1 Documenti soggetti a scansione	36
11.2 Processo di scansione.....	36
12. CONSERVAZIONE DEI DOCUMENTI.....	36
12.1 Struttura dell'archivio	36
12.2 Piano di Conservazione dei documenti.....	37
12.3 Memorizzazione dei documenti analogici, dei documenti informatici e delle rappresentazioni digitali dei documenti cartacei.....	38
12.4 Conservazione dei documenti informatici	38
12.5 Censimento dei depositi documentari, delle banche dati e dei software	39
13. GESTIONE DELL'ARCHIVIO.....	39
13.1 Gli archivi correnti.....	39
13.2 Dall'archivio corrente all'archivio di deposito: il cosiddetto scarto in itinere	39
13.3 Documentazione eliminabile durante lo scarto in itinere	40
13.4 L'archivio di deposito	41
13.5 Dall'archivio di deposito all'archivio storico: lo scarto	43
13.6 Predisposizione della documentazione.....	44

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

13.7	Compilazione elenco documentazione per lo scarto	44
13.8	Frequenza delle operazioni di scarto	45
13.9	Responsabilità sull'osservanza delle norme sullo smaltimento	46
13.10	L'archivio storico.....	46
13.11	Periodi minimi di conservazione	47
13.12	Documentazione a conservazione illimitata	47
13.13	Responsabilità sulla tenuta degli archivi	48
14.	PUBBLICITA' LEGALE E TRASPARENZA AMMINISTRATIVA	48
14.1	Modelli pubblicati	48
14.2	Obblighi di pubblicità trasparenza e diffusione di informazioni	48
14.3	Attuazione del GDPR: gestione dei dati.....	48
15.	ACCESSO	49
15.1	Accessibilità al sistema di protocollo e livelli di riservatezza	49
16.	GESTIONE DELL'EMERGENZA	50
16.1	Misure da adottare in caso di emergenza	51
17.	DISPOSIZIONI FINALI	52
17.1	Norma di rinvio	52
17.2	Approvazione, integrazioni, modifiche ed aggiornamenti del Manuale	52
17.3	Pubblicazione del Manuale.....	52
18.	RIFERIMENTI NORMATIVI.....	53
20.	DOCUMENTI COLLEGATI	55
19.	ALLEGATI.....	55

1. DISPOSIZIONI GENERALI

1.1 ELENCO REVISIONI

N.	Data	Paragrafi modificati	Motivo modifica
0	18.12.2024	Emissione procedura	
1	16.06.2025	Intera procedura	Aggiornamento/revisione

 AGENZIA DI CONTROLLO DEL SISTEMA SOCIO SANITARIO LOMBARDO	 Regione Lombardia	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

1.2 GRUPPO DI LAVORO

Cognome Nome	Qualifica	Struttura di appartenenza	Firmato digitalmente
Alberto Panese	Direttore Struttura Complessa	SC Sanità Digitale e Tecnologie Innovative	Firmato da: ALBERTO PANESE Valido da: 18-01-2024 10:51:53 a: 18-01-2027 02:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale: Marca Temporale (vedi la proprietà della firma) Motivo: Approvo il documento
Andrea De Vitis	Direttore Struttura Complessa	SC Controlli Sanitari e Sociosanitari Integrati	Firmato da: ANDREA DE VITIS Valido da: 22-01-2025 11:28:54 a: 22-01-2028 02:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale: "SigningTime": 25-05-2025 10:40:30 Motivo: Approvo il documento
Davide Archi	Direttore Dipartimento/Struttura Complessa	SC Qualità e Sicurezza delle Cure	Firmato da: DAVIDE ARCHI Valido da: 05-05-2024 09:50:04 a: 05-05-2027 02:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale: "SigningTime": 25-05-2025 14:33:30 Motivo: Approvo il documento
Loredana Nofroni	Direttore Struttura Complessa	SC Appropriatelyzza Gestionale e Organizzativa	Firmato da: LOREDANA ALESSANDRA NOFRONI Motivo: Approvo il documento
Manuela Mineccia	Collaboratore Amministrativo	SC Gestione Affari Istituzionali e Attività Amministrative per le Strutture di Controllo	Firmato da: MANUELA MINECCIA Valido da: 04-08-2024 17:20:58 a: 04-08-2027 02:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale: "SigningTime": 15-06-2025 12:36:10 Motivo: Approvo il documento
Marta Sottoriva	Responsabile Struttura Semplice	SS Bilancio, Programmazione e Acquisti	Firmato da: MARTA SOTTORIVA Valido da: 15-01-2024 10:41:42 a: 15-01-2027 02:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale: Marca Temporale (vedi la proprietà della firma) Motivo: Approvo il documento
Raffaella Botta	Dirigente Amministrativo	Staff Direzione Generale - RPCT	Firmato da: RAFFAELLA BOTTA Valido da: 15-03-2024 10:25:56 a: 15-03-2027 02:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale: Marca Temporale (vedi la proprietà della firma) Motivo: Approvo il documento
Vittorio Russo	Direttore Struttura Complessa	SC Giuridico e Risorse Umane	Firmato da: VITTORIO RUSSO Valido da: 09-04-2025 12:09:37 a: 09-04-2028 02:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale: "SigningTime": 25-05-2025 10:25:40 Motivo: Approvo il documento

Il lavoro è stato coordinato dalla **Dott.ssa Clara Pelliccia**, in qualità di Direttore della “SC Gestione Affari Istituzionali e Attività Amministrative per le Strutture di Controllo”.

1.3 PREMESSA

Tutti i documenti, i fascicoli e gli archivi degli enti pubblici appartengono al patrimonio culturale nazionale, secondo quanto previsto dal Codice dei beni culturali (D.Lgs 22/01/2004 n. 41 artt. 2 e 10); ai sensi dell'art. 822 del Codice civile tali documenti sono soggetti al regime del demanio pubblico e pertanto sono inalienabili.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Tutti i documenti prodotti, ricevuti o conservati a qualsiasi titolo da una Pubblica Amministrazione possiedono fin dall'origine la duplice natura di atti pubblici e di beni culturali. Pertanto, tali atti vanno preservati da ogni alterazione e sottrazione, evitando ogni forma di uso improprio.

Nel corso degli anni, un articolato corpus legislativo, non sempre di facile interpretazione, ha tentato di disciplinare i vari aspetti della gestione documentale, quali la produzione, la conservazione e la trasmissione degli atti (D.P.R. n. 445/2000 e s.m.i.), la tenuta dei documenti informatici (D. L.gs. n. 82/2005 e s.m.i.), l'accesso alle informazioni (L. n. 241/1990 e s.m.i. e D. L.gs. n.33/2013 e s.m.i.) e la tutela dei dati personali e sensibili (D. L.gs. n. 196/2003 e s.m.i.).

Anche la normativa sui beni culturali ha prescritto l'obbligo di garantirne la protezione e la conservazione, l'integrità, la sicurezza e la pubblica fruizione, adottando al contempo tutte le misure idonee “a limitare le situazioni di rischio” (artt. 3, 29 e 30 del D. L.gs. n. 42/2004 e s.m.i.).

I soggetti pubblici detentori di archivi hanno il dovere di collaborare alla loro tutela e valorizzazione (D. L.gs. n. 42/2004, artt. 5 e 7). Agli stessi soggetti è poi attribuito l'obbligo specifico di conservare, ordinare e inventariare i propri archivi, da intendersi come dovere di predisporre mezzi e procedure perché l'archivio corrente nasca ben ordinato, nonché dovere di riordinare l'archivio già esistente ove si trovi in stato di disordine (art. 30, c. 4).

Ogni azione contraria alle norme di buona conservazione dei documenti, ivi compreso il semplice comportamento omissivo o l'abbandono in stato di incuria degli archivi, costituisce una grave violazione di legge.

Pur giovandosi della loro autonomia organizzativa nel creare e ordinare il proprio archivio l'Agenzia è tenuta ad archiviare secondo modalità definite da requisiti normativi e di corretta gestione documentale. In particolare, l'archivio dei documenti di un Ente Pubblico deve soddisfare varie esigenze, definite dal Codice dei beni culturali e del paesaggio, tra cui in particolare:

- essere ordinato (art. 30, comma 4);
- conservato correttamente in sicurezza (art. 30, comma 1);
- senza danni (art. 20, comma 1);
- rispettandone l'integrità (art. 20, comma 2) e l'organicità (art. 30, comma 4);
- curato con idonea manutenzione (art. 29, comma 3);
- restaurato se necessario (art. 29, comma 4);
- non adibito ad usi incompatibili con il suo carattere (art. 20, comma 1).

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

1.4 AMBITO DI APPLICAZIONE

Il presente Manuale di gestione documentale è adottato ai sensi degli articoli 3 e 5 del DPCM 31 ottobre 2000, recante le regole tecniche per il protocollo informatico e descrive il sistema di ricezione, formazione, registrazione, classificazione, fascicolazione, trattamento e conservazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti dell'Agenzia di Controllo del Sistema Socio Sanitario Lombardo (ACSS). In particolare, disciplina:

- le modalità di gestione dei documenti e dei fascicoli dell'Agenzia;
- le modalità per la corretta tenuta dell'archivio dell'ACSS;
- le responsabilità in merito alla conservazione e archiviazione dei documenti cartacei;
- la tempistica di conservazione e le modalità di scarto della documentazione ai sensi del D.Lgs. n. 42/2004 e della DGR X/325 del 27/06/2013, successivamente integrata e modificata mediante approvazione, da ultimo, della versione 04 del Titolario di Classificazione e Massimario di Scarto della Documentazione del Sistema Sanitario e Sociosanitario di Regione Lombardia di cui al Decreto n. 15229 dell'1.12.2017 che costituisce parte integrante e sostanziale della presente procedura operativa (All. 1);
- gli obblighi di pubblicità della trasparenza e l'accesso agli atti, nonché la modalità di trattamento dei dati personali;
- la gestione dell'archivio in caso di emergenza.

Le disposizioni della presente procedura operativa si applicano a tutti i documenti prodotti ed acquisiti dall'ACSS nello svolgimento della propria attività amministrativa.

1.5 DEFINIZIONI GENERALI

Archivio: complesso di documenti prodotti o acquisiti da una Pubblica Amministrazione durante lo svolgimento della propria attività. Si articola in archivio corrente, archivio di deposito, archivio storico, come meglio dettagliato nel successivo art. 3.

Area Organizzativa Omogenea (AOO): insieme definito di unità organizzative di una amministrazione, che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali; in particolare, una AOO utilizza per il servizio di protocollazione un'unica sequenza numerica, rinnovata ogni anno solare.

Assegnazione, individuazione della persona fisica responsabile della trattazione dell'affare o procedimento amministrativo e della gestione dei documenti nella fase corrente.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Autorizzazione allo scarto: Provvedimento emanato dalla Soprintendenza archivistica competente per territorio che autorizza lo scarto, sulla base di una proposta presentata da una P.A.

Casella istituzionale di posta elettronica: la casella di posta elettronica, istituita da un'A OO, per la ricezione dall'esterno e per la spedizione all'esterno dei documenti da registrare a protocollo.

Categoria: la partizione del Titolario, contrassegnata da un simbolo costituito da un numero romano o da un numero arabo o da una lettera dell'alfabeto oppure da un simbolo misto costituito da una lettera e un numero, ecc.

Classificazione: l'operazione che consente di organizzare i documenti in relazione alle funzioni ed alle modalità operative dell'Agenzia.

Conservazione: Attività volta a garantire la tenuta in condizioni idonee, all'interno di archivi analogici e/o digitali, dei documenti.

Copia: la riproduzione di un documento originale eseguita a mano, a macchina o mediante apparecchio per fotocopiare; la semplice copia non ha valore giuridico; la copia ha valore giuridico e si definisce autentica o autenticata quando è emessa da un ente che può rilasciare copie conformi all'originale e reca segni di autenticazione.

Documento amministrativo: il documento amministrativo è la rappresentazione, in qualsiasi modo formata, del contenuto di atti anche interni, dell'ACSS o, comunque, utilizzati ai fini dell'attività amministrativa.

Documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Documento archiviato: il documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica.

Documento conservato: il documento sottoposto al processo di conservazione sostitutiva.

Documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente.

Duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Elenco: la lista con indicazione più o meno sommaria della documentazione compresa in ciascuna busta e dei registri di un fondo non riordinato, secondo l'ordine in cui si trovano le singole unità.

E-mail (posta elettronica): il sistema di comunicazione elettronica attraverso messaggi.

Fascicolazione, l'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Fascicolo: raccolta ordinata, individuata con identificativo univoco, di documenti riuniti per caratteristiche omogenee, in relazione alla natura e alla forma degli stessi, all’oggetto, alla materia o alle funzioni.

Firma digitale, un particolare tipo di firma elettronica avanzata qualificata, basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l’integrità di un documento informatico o di un insieme di documenti informatici.

Firma elettronica avanzata: l’insieme di dati in forma elettronica allegati oppure connessi a un documento informatico, che consentono l’identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

Firma elettronica qualificata: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

Firma elettronica: l’insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

Flusso documentale: il movimento dei documenti all’interno dell’archivio (dalla fase di formazione dell’archivio corrente a quella di conservazione dell’archivio storico).

Gestione dei documenti: l’insieme delle attività finalizzate alla formazione, ricezione, registrazione di protocollo ed alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi, formati o acquisiti dall’Azienda, nell’ambito del sistema di classificazione adottato.

Manuale di gestione dei documenti: il testo che descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta e il protocollo informatico, della gestione dei flussi documentali e degli archivi. Nel caso specifico, trattasi della presente procedura operativa.

Minuta: l’ulteriore esemplare in originale, che resta agli atti dell’ufficio produttore, di un documento già spedito in originale al destinatario o ai destinatari.

Piano di conservazione degli archivi: lo strumento, previsto dalla normativa, che definisce i criteri di organizzazione della documentazione, di selezione periodica e di conservazione permanente dei documenti, redatto e integrato con il sistema di classificazione adottato.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Protocollo informatico: il registro su supporto informatico sul quale vengono registrati quotidianamente i documenti spediti e ricevuti da un ente. La registrazione di protocollo costituisce elemento probante dell'autenticità del documento ed è l'operazione con cui un documento entra a far parte integrante di un archivio e della memoria di un ente, per cui un documento non protocollato è come se non fosse mai stato prodotto o ricevuto. Il protocollo è atto pubblico di fede privilegiata fino a querela di falso; il protocollo è elemento essenziale per la gestione della memoria delle pubbliche amministrazioni in caso di mancanza del numero di protocollo il documento può perdere la sua efficacia.

Protocollo: il numero progressivo automatico apposto a un documento al momento della registrazione nel protocollo informatico.

Scarto: l'operazione con cui si destina al macero una parte della documentazione di un archivio.

Segnatura di protocollo: l'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.

Titolario di classificazione e Massimario di scarto: Strumento archivistico approvato da Regione Lombardia contenente la classificazione e il tempo minimo di conservazione della documentazione amministrativa prodotta in ambito sanitario e sociosanitario (All.1)

1.6 ACRONIMI

ACRONIMO	DESCRIZIONE
ACSS	Agenzia di Controllo del Sistema Socio Sanitario Lombardo
ALL.	Allegato
ANAC	Autorità Nazionale Anticorruzione
CAD	Codice Amministrazione Digitale
CRS	Carta Regionale dei Servizi
D.Lgs	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
GDPR	General Data Protection Regulation (Regolamento generale protezione dati)
PIAO	Piano Integrato di Attività e Organizzazione
RPCT	Responsabile Prevenzione della Corruzione e della Trasparenza
SC	Struttura Complessa
SS	Strutture Semplici
SSD	Strutture Semplici Dipartimentali

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

2. ARTICOLAZIONE E ORGANIZZAZIONE DELLE STRUTTURE

2.1 AREA ORGANIZZATIVA OMOGENEA

Ai fini della gestione dei documenti, l'Agenzia viene considerata come un'unica Area Organizzativa Omogenea (AOO) composta dalle seguenti articolazioni organizzative interne:

- Direzione Generale;
- SC Giuridico e Risorse Umane;
- SC Appropriatelyzza Gestionale e Organizzativa;
- SC Controlli Sanitari e Sociosanitari Integrati;
- SC Sanità Digitale e Tecnologie Innovative;
- SC Qualità e Sicurezza delle cure;
- SC Gestione Affari Istituzionali e Attività Amministrative per le Strutture di Controllo;
- SS Bilancio, Programmazione e Acquisti.

A tale Area è stato assegnato il codice identificativo univoco “AOO: ACE3BB7” e codice IPA: acssl.

2.2 RESPONSABILITÀ DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

La legislazione vigente (D.Lgs. 42/2004), secondo quanto esposto in precedenza, impone ai possessori o detentori di beni culturali di garantire la loro tutela, buona conservazione e sicurezza, evitando ogni situazione di rischio.

L'Agenzia, nella figura del suo Legale Rappresentante, è pienamente responsabile della gestione dei documenti, dalla fase della loro formazione a quella della loro conservazione e dell'accesso agli archivi correnti, anche nel caso in cui le modalità di gestione dovessero comportare l'esternalizzazione di determinati servizi.

Ogni azione amministrativa comporta la produzione, la tenuta e la conservazione di documentazione archivistica: la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi è pertanto responsabile della gestione documentaria in conformità alle disposizioni della presente procedura. Inoltre, gli archivi devono essere ordinati, conservati correttamente in sicurezza, senza danni, rispettandone l'integrità e l'organicità, curati con idonea manutenzione, restaurati se necessario e non adibiti ad usi incompatibili con il loro carattere.

Sull'osservanza della normativa in materia di corretta tenuta degli archivi degli enti pubblici vigila la Soprintendenza Archivistica, organo periferico del Ministero per i Beni e le Attività Culturali. La Soprintendenza può effettuare ispezioni per accertare lo stato di conservazione e di custodia degli archivi e l'osservanza dell'obbligo di dare ordine al proprio archivio (corrente, di deposito e storico);

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

può inoltre fornire assistenza all'Agenzia nella formazione dei piani (o massimari) di conservazione e scarto e dei quadri di classificazione dei documenti, nonché nella definizione delle procedure di protocollazione e archiviazione.

Qualora accertasse situazioni irregolari, pericolose o contrarie alle norme, la Soprintendenza può emettere prescrizioni per la tutela degli archivi, la cui inosservanza è punibile a norma dell'art. 650 del Codice penale, salvo che il fatto non costituisca più grave reato. Se l'Agenzia non provvede alla reintegrazione del danno provocato all'archivio, si può dar luogo all'intervento statale sostitutivo, a spese dell'Agenzia; in caso di urgenza, il Soprintendente può adottare immediatamente le misure conservative necessarie.

In generale, l'esecuzione di opere e lavori di qualunque genere sugli archivi corrente, di deposito o storico dell'Agenzia sono subordinati ad autorizzazione preventiva della Soprintendenza, che può rilasciarla sulla base di un progetto o di una descrizione tecnica dell'intervento, con la facoltà di prescrivere eventuali modifiche o prescrizioni.

2.3 ARTICOLAZIONE DELL'AGENZIA

Ai sensi e nei termini di cui all'organigramma contenuto nel Piano Integrato di Attività e Organizzazione 2024-2025-2026 (PIAO) vigente, l'Agenzia si articola in:

- Strutture Complesse (SC);
- Strutture Semplici Dipartimentali (SSD);
- Strutture Semplici (SS).

2.4 SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Nell'ambito dell'Area Organizzativa Omogenea, ai sensi dell'art. 61, comma 1, del D.P.R. 28 dicembre 2000 n. 445, è individuato un Ufficio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

L'Ufficio ha competenza sulla gestione dell'intera documentazione archivistica, ovunque trattata, distribuita o conservata dall'Agenzia, ai fini della sua corretta registrazione, classificazione, conservazione, selezione e ordinamento.

L'Ufficio ha valenza interna, come supporto all'attività amministrativa, e valenza esterna quale servizio pubblico di accesso alla documentazione, sia per fini amministrativi sia per fini storici e culturali.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Ai sensi del D.Lgs. 22 gennaio 2004 n. 42 e del DPR 445/2000, l'Agenzia individua nell'Archivio una funzione essenziale per garantire la certezza, la semplificazione e la trasparenza dell'agire amministrativo, il reperimento di informazioni affidabili sotto il profilo giuridico, la tutela della memoria storica dell'Agenzia e il diritto di tutti i cittadini all'accesso all'informazione, alla formazione ed allo sviluppo della conoscenza.

L'Archivio e i singoli documenti dell'Agenzia sono beni archivistici; obbediscono pertanto alle disposizioni legislative di cui all'art. 2 e all'art. 10 comma 2, del D.Lgs. n. 42/2004.

L'Archivio, pur nella distinzione delle fasi di vita dei documenti, della loro valenza giuridica e storica e delle suddivisioni, è da ritenersi logicamente unico e funzionalmente integrato.

Alla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi sono affidati i compiti di cui all'art. 61 comma 3 del DPR 445/2000 e DPCM 31/10/2000.

La Struttura competente, in particolare:

- attribuisce e provvede periodicamente ad aggiornare le autorizzazioni per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- garantisce che le operazioni di registrazione di protocollo, classificazione ed indicizzazione dei documenti ricevuti si svolgano nel rispetto delle disposizioni della normativa vigente;
- garantisce la corretta produzione e la conservazione del registro di protocollo di cui all'art. 53;
- cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile in collaborazione con i Sistemi Informativi;
- conserva il registro di emergenza;
- autorizza le operazioni di annullamento e di modifica;
- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali e le attività di gestione degli archivi.

Nell'ambito della gestione dell'Archivio dell'Agenzia, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi:

- coordina e verifica l'attuazione e il rispetto delle procedure adottate nella gestione della documentazione corrente e per il versamento all'Archivio di deposito;
- coordina le operazioni di compilazione e aggiornamento degli strumenti di corredo utili per la

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

gestione e la consultazione delle pratiche depositate;

- sovrintende alle procedure di selezione e scarto dei documenti dell'Archivio di deposito.

La Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi opera d'intesa con il Responsabile della Conservazione dei documenti informatici, ai sensi dell'art. 44 del Codice dell'Amministrazione Digitale (CAD) D.Lgs.7 marzo 2005 n. 82 e ss.mm.e ii.

2.5 UNICITÀ DEL PROTOCOLLO INFORMATICO

Nell'ambito dell'Area Organizzativa Omogenea la numerazione delle registrazioni di protocollo è unica e progressiva, senza distinzione fra i tre i tipi di documenti (“ricevuti”, “spediti” e “interni”).

Essa si chiude al 31 dicembre di ciascun anno solare e ricomincia all'inizio dell'anno successivo. Ciascun documento deve essere identificato mediante l'assegnazione di un unico numero di protocollo e non è consentita l'attribuzione del medesimo numero ad altri documenti, per quanto strettamente correlati tra loro.

2.6 MODELLO OPERATIVO ADOTTATO PER LA GESTIONE DEI DOCUMENTI

Per la gestione dei documenti è adottato un modello operativo di tipo decentrato che prevede la partecipazione di più strutture di protocollazione e uffici utente, abilitati a svolgere soltanto le operazioni di loro competenza.

Il sistema di gestione informatica prevede livelli di accesso differenziati per quanto riguarda l'inserimento, la ricerca e la modifica di dati.

Ad ogni utente è associato un profilo utente che ne identifica la struttura di appartenenza, il nominativo e il livello di accesso a cui è abilitato.

3. FORMAZIONE DEI DOCUMENTI

3.1 MODALITÀ DI FORMAZIONE DEI DOCUMENTI E CONTENUTI MINIMI

Le modalità di formazione dei documenti, la loro struttura, il loro formato e gli altri elementi-base sono determinati dalla Direzione Generale e da quanto previsto dal presente Manuale. Per quanto riguarda i documenti informatici, la loro produzione è regolata sulla base di modelli *standard* presenti nel sistema informatico di gestione documentale.

Il contenuto minimo di ciascun documento deve comunque garantire la presenza delle seguenti informazioni:

- denominazione e logo dell'Agenzia (per quanto riguarda i documenti su supporto cartaceo si utilizza il formato predisposto dall'Agenzia);

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

- indicazione dell'ufficio dell'Agenzia che ha prodotto il documento;
- indirizzo e recapiti completi (via, numero civico, codice avviamento postale, città, sigla della provincia, numero di telefono, numero di fax, indirizzo di posta elettronica dell'Agenzia);
- data: luogo, giorno, mese, anno;
- destinatario;
- oggetto del documento, sufficientemente esaustivo del testo (ogni documento deve trattare un solo oggetto);
- classificazione (categoria, classe, sottoclasse e fascicolo);
- numero degli allegati, se presenti;
- numero di protocollo;
- testo;
- sottoscrizione autografa o elettronico/digitale del Direttore/Dirigente Responsabile (o del funzionario delegato);
- indicazione del Responsabile del procedimento (Legge 7 agosto 1990, n. 241 e ss. mm. e ii.);
- indicazione dello scrittore /referente per la pratica.

3.2 FORMATO DEI DOCUMENTI INFORMATICI

I documenti informatici prodotti dall'Agenzia - quali rappresentazioni informatiche di atti, fatti o dati giuridicamente rilevanti ai sensi dell'art. 1, lett. p) del CAD, indipendentemente dal *software* utilizzato, prima della loro sottoscrizione con firma elettronico/digitale, sono convertiti in uno dei formati *standard* previsti dalla normativa vigente in materia di conservazione, al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione, nonché l'immutabilità nel tempo del contenuto e della struttura.

I documenti ricevuti in un formato diverso da quelli prescritti dal presente Manuale, se sottoscritti con firma digitale sono recepiti dal sistema e convertiti in uno dei formati *standard* previsti. In caso di conversione del formato dei documenti informatici, la corrispondenza fra il formato originale ed il nuovo formato è garantita dal Responsabile della Conservazione dei documenti informatici.

3.3 SOTTOSCRIZIONE DEI DOCUMENTI INFORMATICI

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma elettronico/digitale conforme alle disposizioni di legge.

A tal fine l'Agenzia si avvale dei servizi di certificazione offerti da Regione Lombardia – INFOCERT.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

3.4 VALORE PROBATORIO DEL DOCUMENTO INFORMATICO

Ai sensi dell’art. 20, c. 1-bis del CAD, l’idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità ed immutabilità del documento stesso.

Laddove sottoscritto, il documento informatico ha il valore probatorio di cui all’art. 21 del CAD:

2-bis). Salvo quanto previsto dall’articolo 25, le scritture private di cui all’articolo 1350, primo comma, numeri da 1 a 12, del Codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.

2-ter) Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110, ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Le parti, i fidejacenti, l’interprete e i testimoni sottoscrivono personalmente l’atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti.

5) Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell’economia e delle finanze, sentito il Ministro delegato per l’innovazione e le tecnologie”.

3.5 DOCUMENTI CARTACEI: ORIGINALI, MINUTE E COPIE

Per ogni documento cartaceo destinato ad essere spedito vengono scritti tanti esemplari quanti sono i destinatari.

L’originale è quello spedito al destinatario.

L’originale rappresenta la redazione definitiva, perfetta e autentica negli elementi sostanziali e formali.

L’originale del documento è unico, salvo i casi dove è previsto un originale multiplo (contratti, convenzioni, ecc.).

La minuta rappresenta la redazione definitiva del documento da conservare “agli atti”. Essa porta la firma autografa ed è conservata nel fascicolo del procedimento al quale si riferisce o nell’apposita serie documentaria. Anche sulla minuta è apposta la segnatura di protocollo a cura della struttura emittente.

Qualora si renda necessario, per ragioni amministrative, si possono produrre copie di un medesimo documento. Su ciascuna copia va apposta la dicitura “copia” a cura della struttura.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Le copie trasmesse per ragioni amministrative ad altre strutture organizzative sono conservate per tutto il tempo necessario allo svolgimento del procedimento cui il documento si riferisce e quindi eliminate secondo le norme previste dal Massimario di scarto.

Ai sensi dell'art. 23–ter c. 3 del CAD, le copie informatiche di documenti analogici e le copie per immagine su supporto informatico di documenti analogici *“hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato (...) mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle regole tecniche”* vigenti in materia.

3.6 DOCUMENTI INFORMATICI: ORIGINALI, DUPLICATI E COPIE

Gli atti formati con strumenti informatici, i dati e i documenti informatici, comunque detenuti dall'Agenzia, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, duplicati e copie, nei termini e per gli usi consentiti dalla legge.

Le copie, sia cartacee sia informatiche, di documenti informatici, nonché i duplicati informatici, hanno la stessa efficacia probatoria dell'originale da cui sono tratte, quando la loro conformità all'originale non è espressamente disconosciuta o qualora risulti attestata nelle forme di cui agli artt. 23 e 23-bis del CAD.

Per quanto riguarda la formazione di documenti informatici, il sistema attua un controllo delle versioni dei documenti informatici, tenendo traccia dei loro passaggi e trasformazioni fino alla versione definitiva inviata alla registrazione di protocollo e, ove richiesto, vengono conservate le versioni stesse.

3.7 TUTELA DELLA RISERVATEZZA

I documenti, le banche dati, il protocollo e gli altri registri, sono prodotti in modo da tutelare la riservatezza dei dati personali, dei dati sensibili e dei dati giudiziari secondo la normativa vigente.

4. RICEZIONE DEI DOCUMENTI

4.1 RICEZIONE DEI DOCUMENTI SU SUPPORTO CARTACEO

I documenti su supporto cartaceo possono pervenire all'Area Organizzativa Omogenea, presso la sede dell'Agenzia attraverso una delle seguenti modalità:

- posta (ordinaria, raccomandata, celere, corriere espresso, ecc.);
- a mano.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

La corrispondenza indirizzata genericamente all' Agenzia di Controllo del sistema Socio Sanitario oppure a specifici Dipartimenti dell'Agenzia o ai singoli dipendenti, viene aperta, timbrata con la data del giorno corrente, suddivisa per tipologie, e quindi consegnata agli uffici preposti alla protocollazione.

Gli Atti Giudiziari e i telegrammi vengono consegnati in busta chiusa all'Ufficio Protocollo o alle unità di protocollazione decentrate, per la registrazione ed il seguito di competenza.

I meri avvisi di avvenuto recapito di un telegramma vengono semplicemente timbrati col timbro di arrivo e smistati ai destinatari.

La posta indirizzata al Direttore Generale dell'Agenzia viene aperta dall'Ufficio responsabile della gestione del protocollo in entrata e successivamente valutata ai fini dell'individuazione di eventuali precedenti e della protocollazione da effettuarsi a cura dell'Ufficio stesso.

La corrispondenza indirizzata ai Direttori che riporta la dicitura “riservata” o “personale” o simili viene trattata secondo quanto previsto al successivo punto 6.3.

Gli inviti, le note augurali e le informazioni pubblicitarie, ove esternamente riconoscibili dal plico, sono mantenuti nella loro busta, timbrata con il timbro di arrivo.

4.2 RICEZIONE DEI DOCUMENTI INFORMATICI

I documenti informatici possono pervenire all'Area Organizzativa Omogenea, presso la sede dell'Agenzia, attraverso:

- spedizione via posta elettronica normale o certificata;
- trasmissione su supporto rimovibile (ad es.: Cd-Rom, DVD, pen-drive, ecc.).

La ricezione dei documenti informatici è assicurata tramite:

- casella dell'Agenzia di posta elettronica istituzionale: direzione@acsslombardia.it
- casella dell'Agenzia di posta elettronica certificata (PEC): acss@pec.regione.lombardia.it

I suddetti indirizzi sono riservati alla funzione di ricezione/spedizione, sono resi disponibili agli uffici preposti alla registrazione di protocollo e sono pubblicati sul sito Internet dell'Agenzia all'indirizzo: Agenzia di Controllo del Sistema Socio Sanitario Lombardo - www.acsslombardia.it

I documenti informatici eventualmente pervenuti alle unità organizzative non abilitate alla ricezione devono essere inoltrati all'indirizzo di posta elettronica istituzionale indicato dall'Agenzia come deputato alle operazioni di registrazione.

Per quanto riguarda la gestione della posta elettronica si veda quanto previsto alla Sezione 7.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

4.3 RICEVUTE ATTESTANTI LA RICEZIONE DEI DOCUMENTI

La ricevuta della consegna di un documento cartaceo, laddove richiesta, è costituita dalla fotocopia del primo foglio del documento stesso, con un timbro che attesti il giorno della consegna. Per la corrispondenza consegnata in portineria, viene timbrata la bolletta di consegna con timbro datario e firma dell'addetto ricevente.

Per altri tipi di documenti analogici verrà rilasciata ricevuta tramite apposita dichiarazione.

Nel caso di ricezione dei documenti informatici, la notifica al mittente dell'avvenuto ricevimento è assicurata dal sistema elettronico.

4.4 CONSERVAZIONE DELLE BUSTE O ALTRI CONTENITORI DI DOCUMENTAZIONE

Le buste dei documenti pervenuti si inoltrano sempre agli uffici destinatari e vengono conservate almeno per 24 ore; laddove necessario per espressa disposizione normativa o altrimenti ritenuto opportuno dal Responsabile dell'ufficio assegnatario, le stesse possono essere conservate per periodi più lunghi.

4.5 ORARI DI APERTURA PER IL RICEVIMENTO DELLA DOCUMENTAZIONE CARTACEA

L'Ufficio postale di Palazzo Sistema è collocato in via Taramelli 26, Nucleo G, Piano 0. Il numero interno a cui risponde è il seguente: 22589.

L' e-mail dell'Ufficio postale di riferimento è: puntoposta_palazzosistema@regione.lombardia.it.

L'Ufficio postale è aperto dal lunedì al venerdì dalle ore 9 alle ore 12.30 e dalle ore 14.30 alle ore 16:30.

5.REGISTRAZIONE DEI DOCUMENTI

5.1 DOCUMENTI RICEVUTI, SPEDITI, INTERNI

In relazione alle modalità di produzione, ricezione o acquisizione al patrimonio documentale dell'Agenzia, i documenti si distinguono in:

- documenti ricevuti (In Arrivo);
- documenti spediti (In Uscita);
- documenti interni, informali e formali.

Documenti ricevuti (in Arrivo)

I documenti ricevuti sono tutti i documenti ricevuti dall'Agenzia, provenienti da soggetti (persone fisiche o persone giuridiche, pubbliche e private) esterni.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Documenti spediti (in Uscita)

I documenti spediti sono tutti i documenti prodotti dall'Agenzia e destinati, per competenza, a soggetti esterni (persone fisiche o giuridiche).

Documenti interni

I documenti interni sono prodotti, mantenuti e destinati, per competenza, ad altri uffici interni all'Agenzia.

I documenti interni si distinguono in:

- informali: di norma sono documenti di lavoro di natura non ufficiale, temporanea e/o interlocutoria, a preminente carattere informativo/operativo/preparatorio (ad es.: scambio di prime bozze di documenti senza annotazioni significative, convocazioni e verbali di incontri interni ad un ufficio o comunque non caratterizzati da particolare ufficialità, memorie informali, brevi appunti, indicazioni operative del Dirigente interessato, ecc...).
- formali: sono quei documenti aventi rilevanza giuridico-probatoria, di norma redatti dal personale nell'esercizio delle proprie funzioni ed al fine di documentare fatti inerenti all'attività svolta ed alla regolarità dell'azione dell'Agenzia o qualsiasi altro documento dal quale possano nascere diritti, doveri, o legittime aspettative di terzi.

5.2 DOCUMENTI SOGGETTI A REGISTRAZIONE DI PROTOCOLLO

Tutti i documenti prodotti e ricevuti dall'Agenzia, sia analogici che informatici, sono registrati al protocollo in dotazione all'Agenzia, ad eccezione di quelli indicati successivamente (punto 5.3 e Sezione 6).

Salvo quanto previsto nella successiva Sezione 6, sono eliminati tutti i sistemi di registrazione dei documenti alternativi al protocollo informatico.

5.3 DOCUMENTI NON SOGGETTI A REGISTRAZIONE OBBLIGATORIA DI PROTOCOLLO

Ai sensi dell'articolo 53, comma 5, del DPR 445/2000, sono esclusi dalla registrazione di protocollo:

- gazzette ufficiali, bollettini ufficiali, notiziari della pubblica amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, stampe varie, plichi di libri, depliant;
- biglietti augurali, inviti a manifestazioni e documenti di occasione vari che non attivino

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

procedimenti amministrativi.

Non sono inoltre soggetti a registrazione di protocollo i documenti interni informali come definiti al precedente punto 5.1.

5.4 REGISTRAZIONE DI PROTOCOLLO DEI DOCUMENTI

La registrazione di protocollo di un documento è eseguita dopo averne verificato l'autenticità, la provenienza e l'integrità.

La registrazione dei documenti ricevuti, spediti e interni è effettuata in un'unica operazione, utilizzando le apposite funzioni previste dal sistema di protocollo (In Arrivo, In Uscita, Interno).

I requisiti necessari di ciascuna registrazione di protocollo sono:

- numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e numero di protocollo dei documenti ricevuti, se disponibili;
- impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;
- identificativo di chi ha protocollato il documento e ufficio di appartenenza;
- classificazione (vedi Titolario di classificazione All.1);
- assegnazione;
- data di arrivo;
- allegati.

Inoltre, possono essere aggiunti:

- estremi provvedimento differimento termini di registrazione;
- mezzo di ricezione/spedizione (lettera ordinaria, prioritaria, raccomandata, corriere, ecc.);
- tipo documento;
- livello di riservatezza;
- elementi identificativi del procedimento amministrativo, se necessario;
- eventuali altre informazioni connesse al documento.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Una volta salvato il *report* di protocollazione, il sistema genera automaticamente un numero progressivo, che rappresenta il numero di protocollo attribuito al documento.

Il numero progressivo di protocollo è un numero ordinale costituito da almeno sette cifre numeriche.

L'insieme delle registrazioni effettuate costituisce il *Registro di protocollo*, che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

Il Registro di protocollo si configura come *atto pubblico di fede privilegiata*; da ciò deriva che il dipendente dell'Agenzia che opera nel sistema di protocollazione assume la qualità di pubblico ufficiale; chiunque intenda contestare la veridicità di una o più registrazioni contenute nel protocollo dell'Agenzia è tenuto a proporre querela di falso in base all'art. 221 del Codice di procedura civile.

5.5 SEGNATURA DI PROTOCOLLO

La segnatura di protocollo apposta o associata al documento è effettuata contemporaneamente alla registrazione di protocollo con apposito timbro datario d'arrivo.

I requisiti necessari di ciascuna segnatura di protocollo sono:

- codice identificativo dell'Agenzia;
- codice identificativo dell'Area Organizzativa Omogenea;
- data di protocollo;
- numero di protocollo (anteponendo al numero ordinale una successione di simboli “zero”, fino a costituire le sette cifre richieste);
- indice di classificazione;

per i documenti informatici trasmessi ad altre pubbliche amministrazioni attraverso sistemi di interoperabilità, i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un *file* conforme alle specifiche dell'*Extensible Markup Language* (XML) e compatibile con il *Document Type Definition* (DTD) e comprendono anche:

- persona o ufficio destinatari.

5.6 ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

Le registrazioni di protocollo in entrata e in uscita non possono essere modificate o annullate da parte della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

5.7 DIFFERIMENTO DEI TERMINI DI REGISTRAZIONE

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata da parte delle unità di protocollazione abilitate e comunque non oltre le quarantotto ore lavorative dal ricevimento dei medesimi, conferendo la Scheda di ricevuta protocollo.

Eccezionalmente, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi può autorizzare la registrazione in tempi successivi, fissando comunque un limite di tempo entro il quale devono essere protocollati e, in caso di scadenze predeterminate, conferendo valore, attraverso una dichiarazione, al timbro datario apposto sui documenti di cui si è differita la registrazione.

5.8 REGISTRO GIORNALIERO E ANNUALE DI PROTOCOLLO

Il contenuto del registro e del sistema di protocollo informatico alla fine di ogni giorno è salvato su supporti di memorizzazione.

Dalle registrazioni del protocollo informatico è sempre possibile estrarre evidenza analogica.

5.9 REGISTRO DI EMERGENZA

Nel caso di inconvenienti tecnici che dovessero verificarsi sui collegamenti telematici o comunque sul funzionamento del sistema di protocollo, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento delle operazioni di protocollo su un registro di emergenza.

6. CASI PARTICOLARI

6.1 DOCUMENTAZIONE SOGGETTA A REGISTRAZIONE PARTICOLARE

L'elenco delle tipologie documentarie sottoposte a registrazione particolare viene aggiornato annualmente su iniziativa della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi.

I *software* di produzione e conservazione di questa tipologia particolare di documentazione devono consentire di eseguire su di essa tutte le operazioni previste nell'ambito della gestione dei documenti e del sistema adottato per il protocollo informatico. Ogni registrazione deve riportare necessariamente:

- dati identificativi di ciascun atto (autore, destinatario, oggetto, data);
- dati di classificazione;
- numero di repertorio progressivo e annuale.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

6.2 DOCUMENTAZIONE DI GARE D’APPALTO

L’Agenzia di Controllo del Sistema Socio-Sanitario lombardo, in relazione delle modeste dimensioni dell’Ente, per garantire il corretto funzionamento della gestione operativa si approvvigiona di beni e servizi, di norma, tramite procedure di affidamento i cui importi risultano di modica entità e principalmente inferiori alle soglie comunitarie di cui all’art. 14 comma 1 lettera c) del D.Lgs. n. 36/2023.

I documenti relativi alle procedure svolte sui portali telematici delle Centrali di Committenza (Consip e ARIA) e quelli pervenuti in modalità elettronica sono inseriti nel sistema di gestione documentale. Per gli affidamenti inferiori a euro 5 mila, qualora non gestiti tramite portale, e non vi sia la possibilità di riversare i file della documentazione di gara direttamente nel sistema di gestione documentale, la SS Bilancio, Programmazione e Acquisti provvede a scaricarli e inserirli manualmente nei rispettivi fascicoli.

6.3 DOCUMENTI A CARATTERE RISERVATO, PERSONALE E /O CONFIDENZIALE

La corrispondenza indirizzata nominativamente al personale viene regolarmente aperta e registrata a protocollo, a meno che sulla busta non sia riportata la dicitura “riservata” o “personale” o simili. In questo caso, viene recapitata in busta chiusa al destinatario il quale, dopo averla aperta, se valuta che il contenuto del documento ricevuto non è personale, lo consegna alla più vicina unità di protocollazione, per la registrazione di protocollo.

6.4 LETTERE ANONIME

Le lettere anonime indirizzate alla Direzione Generale dell’ACSS non vengono registrate dall’Ufficio Protocollo ma sono attenzionate dalla Direzione Generale stessa che ne valuta sia in termini di protocollazione sia di eventuale seguito.

6.5 DOCUMENTI CON FIRMA ILLEGGIBILE

I documenti ricevuti con firma illeggibile e di cui non è identificabile l’autore, vengono protocollati indicando nel campo mittente la dicitura “mittente non identificabile” e sono inoltrati alle strutture competenti. Il responsabile del procedimento ricevuto il documento valuterà la possibilità nonché la necessità di acquisire gli elementi mancanti per perfezionare l’atto, provvedendo altresì a comunicare all’Ufficio Protocollo il nominativo del mittente per le opportune modifiche.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

6.6 DOCUMENTI NON FIRMATI

I documenti ricevuti privi di firma, ma il cui mittente è comunque chiaramente identificabile, vengono protocollati e inoltrati agli uffici responsabili del procedimento, che valuteranno la necessità di acquisire la dovuta sottoscrizione per il perfezionamento degli atti.

6.7 CORRISPONDENZA CON PIÙ DESTINATARI

Tutte le comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo. Nei protocolli in Uscita o Interni con una pluralità di destinatari tale da non poter essere contenuta nell'apposito campo dell'applicativo, dovrà essere inserita la dicitura “Destinatari diversi – vedi elenco”. L'elenco dei destinatari deve essere unito al documento e registrato nel sistema di protocollo. Sull'elenco si riporta la segnatura di protocollo.

6.8 ALLEGATI

Tutti gli allegati devono pervenire alle unità di protocollazione, per la registrazione, unitamente ai documenti a cui si accompagnano.

Su ogni allegato è riportato il timbro della segnatura di protocollo.

Si annota sia sulla lettera sia nella registrazione di protocollo, l'eventuale mancanza degli allegati.

6.9 DOCUMENTAZIONE DI COMPETENZA DI ALTRE AMMINISTRAZIONI O DI ALTRI SOGGETTI

Qualora pervenga all'Agenzia un documento di competenza di un'altra amministrazione o destinato ad altra persona fisica o giuridica, lo stesso viene trasmesso a chi di competenza, se individuabile, con lettera protocollata di accompagnamento, altrimenti viene restituito al mittente.

Se il documento viene erroneamente protocollato, il numero di protocollo deve essere annullato e il documento inviato al destinatario, con nota accompagnatoria protocollata.

6.10 DOCUMENTI ORIGINALI PLURIMI O IN COPIA PER CONOSCENZA

Ai documenti originali plurimi, o copie dello stesso documento, si attribuirà un unico numero di protocollo e, successivamente, originali e/o copie si assegneranno ai singoli destinatari.

6.11 OGGETTI PLURIMI

Qualora un documento in entrata presenti più oggetti, relativi a procedimenti diversi e pertanto da assegnare a più fascicoli, si dovranno produrre copie autentiche dello stesso documento e successivamente registrarle, classificarle e fascicolarle indipendentemente una dall'altra.

L'originale verrà inviato al destinatario indicato nel documento, oppure, nel caso di destinatari plurimi, al primo in indirizzo.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

6.12 PRODUZIONE SERIALE DI DOCUMENTI SULLA BASE DI UN MODELLO GENERALE

Nel caso di produzione in serie di documenti-base che abbiano destinatari multipli e parti minime variabili di contenuto (quali la diversità di importi, date, ecc.), dovranno essere compilati gli elenchi dei destinatari e delle parti variabili dei documenti-base ad essi riferiti.

Gli elenchi devono essere conservati insieme al documento-base nel fascicolo. Il documento-base, ossia minuta/copia per atti, deve essere firmato in autografo o con firma digitale.

Per quanto riguarda la protocollazione si potrà inserire nel campo del destinatario la dicitura “Destinatari diversi – vedi elenco”.

Sui documenti inviati ai destinatari, ai quali non si vuole apporre singolarmente la sottoscrizione, dovrà essere obbligatoriamente riportata l'indicazione del nominativo del sottoscrittore, preceduto dall'abbreviazione “F.to”, e dalla seguente dicitura: *“L'originale del documento è conservato presso (indicare la Struttura). La firma autografa/digitale è sostituita dall'indicazione del nome a norma dell'art. 3 comma 2, del D.Lgs. 39/1993”*.

6.13 MODELLI PUBBLICATI

Ai sensi dell'art. 57 del CAD e dell'art. 6 del D.L. 13 maggio 2011, n. 70 (convertito con Legge 12 luglio 2011, n. 106), l'Agenzia si impegna a rendere disponibili per via telematica l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.

Non può essere richiesto l'uso di moduli e formulari che non siano stati pubblicati e, in caso di omessa pubblicazione, i relativi procedimenti possono essere avviati anche in assenza dei suddetti moduli o formulari. Altri atti o documenti potranno essere richiesti solo se strettamente necessari e la loro mancanza non potrà costituire in ogni caso motivo di rigetto dell'istanza.

Tutti i modelli di documenti pubblicati sul sito Internet o sulla rete Intranet dell'Agenzia sono classificati secondo il Titolario di classificazione in uso.

6.14 TRASMISSIONI TELEMATICHE

I flussi documentali sono trasmessi/ricevuti dall'Agenzia con immissione diretta dei dati sul server dell'Ente destinatario, senza la produzione e conservazione dell'originale cartaceo.

Anche laddove non vengano trasmessi con firma digitale e sistema di crittografia, tali documenti sono comunque sempre inviati tramite linee di comunicazione sicure, riservate e ad identificazione univoca, attivate con i singoli Enti destinatari.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione. Per quanto concerne la conservazione della documentazione digitale, si rimanda al Titolario e Massimario di scarto (All.1), al Piano di Conservazione (All.3) e al Regolamento per la Politica della Sicurezza delle Informazioni e la Cyber Security di ACSS (All.6).

6.15 DOCUMENTAZIONE GESTIONALE INTERNA

Angolo del dipendente

I documenti gestionali interni (ferie, permessi, ecc...) presentati dai dipendenti, non vengono protocollati in quanto sono registrati nell'apposito *software* gestionale (Istruzioni Operative “Angolo del dipendente”).

L'eventuale documentazione cartacea viene conservata in fascicoli specifici gestionali o nel fascicolo personale.

7. GESTIONE DELLA POSTA ELETTRONICA

La posta elettronica può essere utilizzata per l'invio di comunicazioni e per l'invio di documenti, sia all'interno dell'Agenzia sia nei rapporti con i cittadini ed altri soggetti privati, sia con altre Pubbliche Amministrazioni, ai sensi del Capo IV del CAD.

Le comunicazioni e i documenti, trasmessi e ricevuti per posta elettronica, formano oggetto di registrazione di protocollo e sono validi ai fini del procedimento amministrativo, una volta che ne sia accertata la provenienza ai sensi dell'art. 40-bis del CAD.

Le comunicazioni informali ricevute o trasmesse per posta elettronica, che consistano in semplice scambio di informazioni che non impegnino l'Agenzia verso terzi, non sono protocollate. A chi ne fa richiesta deve sempre essere data la risposta dell'avvenuto ricevimento.

La posta elettronica individuale/nominativa non può essere utilizzata per la ricezione o la spedizione di documenti a firma digitale, per i quali è prevista una apposita casella ufficiale.

È vietato l'utilizzo di tale casella per comunicazioni non attinenti all'attività dell'Agenzia.

Nel formato dei messaggi di posta elettronica non certificata diretti all'esterno è inserito automaticamente il seguente testo: *“Rispetta l'ambiente. Non stampare questa mail se non è necessario. Il presente messaggio contiene informazioni di natura professionale attinente alla attività lavorativa. Ai fini dello svolgimento dell'attività lavorativa le eventuali risposte potranno essere conosciute da altri soggetti nell'ambito dell'organizzazione del mittente. Le informazioni contenute in questa comunicazione sono riservate e destinate esclusivamente alla/e persona/e/o all'ente/i sopra indicati. È vietato ai soggetti diversi dai destinatari qualsiasi uso, copia, diffusione di quanto in esso*

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

contenuto ai sensi del codice in materia di protezione dei dati personali (D. Lgs. 30 giugno 2003, n. 196). L’Agenzia di Controllo del Sistema Sociosanitario Lombardo declina ogni responsabilità per errori, omissioni, virus contenuti in questo messaggio o nel suo allegato che risultassero dalla trasmissione. Se questa comunicazione Vi fosse pervenuta per errore, Vi preghiamo di rispondere a questa mail e successivamente cancellarla dal Vostro sistema. grazie”.

7.1 LA POSTA ELETTRONICA NELLE COMUNICAZIONI INTERNE ALL’AGENZIA

Ai sensi dell’art. 47 comma 3 del CAD, le comunicazioni tra l’Agenzia e i dipendenti, nonché tra i vari uffici dell’Agenzia, avvengono, di norma, mediante l’utilizzo della casella di posta elettronica istituzionale dei singoli uffici, nel rispetto delle norme di protezione in materia dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

La posta elettronica viene utilizzata per:

- convocare riunioni (interne all’Agenzia);
- inviare comunicazioni di servizio o notizie dirette ai dipendenti in merito a informazioni generali di organizzazione;
- diffondere circolari e ordini di servizio (gli originali si conservano nel fascicolo specifico);
- diffondere rappresentazioni digitali di documenti cartacei regolarmente classificati e protocollati (l’originale debitamente sottoscritto si conserva nel fascicolo specifico). In tal caso, i documenti acclusi al messaggio sono trasmessi in copia immagine in formato “.pdf”.

7.2 LA POSTA ELETTRONICA NELLE COMUNICAZIONI VERSO L’ESTERNO (PUBBLICHE AMMINISTRAZIONI, CITTADINI E ALTRI SOGGETTI PRIVATI)

Le comunicazioni formali e la trasmissione via posta elettronica di documenti, il cui contenuto impegna l’Agenzia verso terzi, devono sempre essere effettuate con posta elettronica istituzionale o posta elettronica certificata istituzionale.

Il documento inviato:

- se originariamente informatico, dovrà essere sottoscritto con firma elettronica avanzata, qualificata o digitale, ai sensi dell’art. 21 comma 2-bis del CAD;
- se originariamente analogico (cartaceo) dovrà esserne trasmessa una copia per immagine su supporto informatico, attestandone la conformità all’originale analogico mediante l’utilizzo di firma digitale o firma elettronica qualificata, ai sensi dell’art. 23-ter del CAD; nei casi in cui il documento venga trasmesso tramite Posta Elettronica Certificata ad un’altra pubblica amministrazione, non sono richieste né l’attestazione di conformità all’originale né la firma

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

digitale o altro tipo di firma elettronica qualificata, secondo quanto disposto dall’art. 47 comma 2 lett. d) del CAD.

7.3 LA POSTA ELETTRONICA RICEVUTA DA CITTADINI O ALTRI SOGGETTI PRIVATI

Ai sensi dell’art. 65 comma 1 del CAD, le istanze e le dichiarazioni trasmesse per via telematica all’indirizzo istituzionale dell’Agenzia devono ritenersi valide a tutti gli effetti di legge, qualora:

- siano trasmesse, via posta elettronica o via posta elettronica certificata, regolarmente sottoscritte con firma digitale dotata di certificato valido rilasciato da un certificatore accreditato;
- l’autore del documento è identificato dal sistema informatico con l’uso della carta d’identità elettronica o della Carta Regionale dei Servizi (CRS) oppure attraverso altri strumenti informatici messi a disposizione dall’Agenzia, che consentano l’individuazione certa del soggetto richiedente;
- siano inviate utilizzando una casella di Posta Elettronica Certificata, le cui credenziali di accesso siano state rilasciate previa identificazione del titolare attestata da parte del gestore del sistema;
- si tratti di istanze o dichiarazioni sostitutive di atto di notorietà trasmesse secondo le modalità di cui all’art. 38 comma 3 del DPR 445/2000.

Al di fuori delle predette ipotesi, le comunicazioni di posta elettronica che pervengono all’indirizzo istituzionale dell’Agenzia o di singole Strutture dell’Agenzia, sono valutate in ragione della loro rispondenza a ragionevoli criteri di attendibilità e riconducibilità al mittente dichiarato, e successivamente soggette, se del caso, a protocollazione secondo le seguenti modalità:

- messaggi di posta elettronica con allegate rappresentazioni digitali di documenti originali cartacei: nel caso in cui via posta elettronica pervengano rappresentazioni digitali di documenti originali cartacei in uno dei seguenti formati standard TIFF, PDF, PDF-A, JPEG, la rappresentazione digitale e il messaggio che la trasmette verranno stampati su carta e la rappresentazione digitale verrà protocollata; nel caso si tratti di istanze o dichiarazioni sostitutive di atto di notorietà, dovrà anche essere obbligatoriamente prodotta copia per immagine del documento di identità del sottoscrittore, ai sensi dell’art. 65 del CAD e dell’art. 38 comma 3 del DPR 445/2000.
- messaggi di posta elettronica senza allegati: qualora si volessero registrare al protocollo semplici messaggi di posta elettronica, il Responsabile del procedimento deve richiederne la protocollazione, dichiarandone per iscritto la provenienza.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

In ogni caso, spetterà al Responsabile del procedimento, ove ne rilevi la necessità, richiedere al mittente la regolarizzazione dell'istanza o della dichiarazione, acquisendo ogni utile documentazione integrativa, compresa la firma autografa del documento.

7.4 LA POSTA ELETTRONICA RICEVUTA DA ALTRE PUBBLICHE AMMINISTRAZIONI

Ai sensi dell'art. 47 del CAD, le comunicazioni e i documenti ricevuti da altre Pubbliche amministrazioni, attraverso l'utilizzo della posta elettronica, sono valide ai fini del procedimento una volta che ne sia verificata la provenienza ovvero quando:

- sono sottoscritti con firma elettronica qualificata o digitale;
- sono dotati di segnatura di protocollo;
- sono trasmessi attraverso sistemi di posta elettronica certificata;
- sono trasmesse attraverso sistemi di interoperabilità di protocollo informatico o altri sistemi idonei ad attestarne inequivocabilmente la provenienza.

8. ASSEGNAZIONE E CLASSIFICAZIONE DEI DOCUMENTI

8.1 ASSEGNAZIONE

Il Dirigente Responsabile interessato che riceve il documento provvede ad assegnare a sé o ad un proprio collaboratore ovvero ad un ufficio sotto ordinato, la responsabilità del procedimento connesso al documento.

L'operazione di assegnazione è effettuata attraverso l'applicativo di protocollo.

Fino a quando non sia effettuata la predetta assegnazione, è considerato Responsabile del procedimento il Dirigente responsabile interessato che riceve il documento.

Le abilitazioni all'assegnazione dei documenti tramite il sistema informatico di gestione documentale sono rilasciate dal Responsabile del Servizio protocollo informatico, della gestione dei flussi documentali e degli archivi.

8.2 MODIFICA DELLE ASSEGNAZIONI

Nel caso di un'assegnazione errata, l'ufficio dell'Agenzia che riceve il documento è tenuto a trasmetterlo, nel più breve tempo possibile, all'unità di protocollazione che ha effettuato l'assegnazione, la quale provvederà alla riassegnazione, correggendo le informazioni inserite nel sistema informatico ed inviando il documento all'ufficio di competenza.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Il sistema di gestione informatica dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua le operazioni sopra descritte, con la data e l'ora di esecuzione.

8.3 CONSEGNA DEI DOCUMENTI CARTACEI

Esauriti gli adempimenti di cui ai precedenti punti, i documenti cartacei, protocollati e assegnati, e la posta che non necessita di protocollazione, sono resi disponibili ai destinatari nei modi seguenti:

- l'Ufficio postale avvisa la Direzione Generale via e-mail o telefono dell'arrivo della posta, la Segreteria provvede al ritiro e consegna direttamente agli interessati;
- mediante ritiro diretto, presso l'Ufficio postale, da parte degli operatori degli uffici della Sede centrale.

8.4 CONSEGNA DEI DOCUMENTI INFORMATICI

I documenti informatici e/o le immagini digitali dei documenti cartacei acquisite con lo *scanner* sono resi disponibili agli uffici o ai responsabili di procedimento tramite il sistema informatico di gestione documentale.

8.5 CLASSIFICAZIONE DEI DOCUMENTI

Tutti i documenti ricevuti o prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al Titolario di classificazione (Allegato n.1), anche se non sono protocollati.

La classificazione dei documenti in arrivo è effettuata dalle unità di protocollazione abilitate; la classificazione dei documenti in partenza è effettuata dagli uffici produttori.

Sono classificati anche gli atti preparatori interni, le minute o altri documenti che non vengono protocollati o siano soggetti a registrazione particolare.

Il programma di protocollo informatico non permette la registrazione di documenti non classificati.

9. FASCICOLAZIONE DEI DOCUMENTI

9.1 FORMAZIONE E IDENTIFICAZIONE DEI FASCICOLI

Tutti i documenti, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli o serie documentarie.

L'apertura di un nuovo fascicolo è effettuata dalla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi su richiesta dei Responsabili interessati.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

La formazione di un nuovo fascicolo avviene attraverso l'operazione di apertura, con richiesta scritta, che prevede la registrazione sul repertorio/elenco dei fascicoli e nel sistema informatico delle seguenti informazioni:

- categoria, classe e sottoclassi del Titolario di classificazione;
- numero del fascicolo (la numerazione dei fascicoli è annuale per ogni classe);
- oggetto del fascicolo;
- data di apertura;
- ufficio a cui è assegnato;
- responsabile del procedimento;
- livello di riservatezza;
- tempo di conservazione.

Il sistema di protocollo informatico provvede automaticamente ad aggiornare il repertorio/elenco dei fascicoli sulla base del Piano di Fascicolazione (vedi All.4).

Entro il mese di dicembre di ogni anno la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi provvede a formulare, sulla base del Titolario di classificazione (All.1), di concerto con gli uffici dell'Agenzia, il piano della fascicolazione per l'anno successivo.

9.2 PROCESSO DI FORMAZIONE DEI FASCICOLI

In presenza di un documento da inserire in un fascicolo si stabilisce, consultando le funzioni del protocollo informatico o il repertorio dei fascicoli, se esso si colloca nell'ambito di un affare o procedimento in corso, oppure se dà avvio ad un nuovo procedimento; se il documento deve essere inserito in un fascicolo già aperto, dopo la classificazione e protocollazione viene rimesso al Responsabile del procedimento, che ha cura di inserirlo nel fascicolo; se invece dà avvio a un nuovo affare, si apre un nuovo fascicolo (con le procedure sopra descritte).

Nel caso di documenti informatici, il sistema provvede automaticamente, dopo l'assegnazione del numero di fascicolo, a inserire il documento nel rispettivo fascicolo informatico.

Qualora si riceva un documento analogico da inserire in un fascicolo informatico, sarà cura della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi produrre la copia digitale conforme del documento stesso, in ottemperanza alle norme in materia di riproduzione sostitutiva. L'originale cartaceo sarà conservato dall'Ufficio Responsabile nella gestione del protocollo.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

I documenti prodotti dall’Agenzia sono fascicolati da chi li scrive; pertanto perverranno alle unità di protocollazione già con l’indicazione del numero/identificativo di fascicolo.

I codici alfanumerici di fascicolazione sono riportati su tutti i documenti.

Qualora si riceva un documento informatico da inserire in un fascicolo analogico, il fascicolo sarà composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti ad un affare o procedimento amministrativo che dà origine a due unità archivistiche di conservazione differenti; l’unitarietà del fascicolo è garantita dal sistema mediante l’indice di classificazione e il numero di repertorio. Per la fascicolazione dei documenti dell’Agenzia di rimanda all’allegato n. 4 *“Piano di Fascicolazione”*.

9.3 MODIFICA DELLE ASSEGNAZIONI DEI FASCICOLI

La riassegnazione di un fascicolo è effettuata dall’Ufficio Responsabile nella gestione del protocollo, su istanza scritta dell’interessato che ha in carico il fascicolo, provvedendo a correggere le informazioni del sistema informatico e del repertorio dei fascicoli ed inoltrando successivamente il fascicolo al Responsabile del procedimento di nuovo carico.

Delle operazioni di riassegnazione e degli estremi del provvedimento di autorizzazione è lasciata traccia nel sistema informatico di gestione dei documenti.

9.4 TENUTA DEI FASCICOLI DELL’ARCHIVIO CORRENTE

I fascicoli dell’Archivio corrente sono gestiti a cura dei Responsabili interessati e conservati presso gli uffici di competenza fino al trasferimento nell’Archivio di deposito.

Per quanto riguarda i fascicoli informatici, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi, d’intesa con il Responsabile della Conservazione dei documenti informatici, provvede al loro trasferimento in archivi informatici di conservazione.

9.5 SCAMBIO DI DOCUMENTI O DI FASCICOLI FRA GLI UFFICI DELL’AGENZIA

Della comunicazione/scambio di informazioni, di documenti o di unità archivistiche giuridicamente rilevanti all’interno dell’Agenzia, deve essere tenuta traccia nel sistema informatico di gestione dei documenti.

10. SPEDIZIONE DEI DOCUMENTI DESTINATI ALL’ESTERNO

10.1 SPEDIZIONE DEI DOCUMENTI CARTACEI

I documenti da spedire devono essere completi di firma autografa, di classificazione e del numero di fascicolo, nonché degli elementi previsti dalla normativa sul procedimento amministrativo.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

La corrispondenza è imbustata a cura degli uffici produttori e convogliata agli uffici preposti alle operazioni di affrancatura e spedizione.

Nel caso di spedizione che utilizzi pezze di accompagnamento (raccomandate, posta celere, corriere o altro mezzo di spedizione), queste devono essere compilate a cura dell'ufficio produttore, secondo le procedure in atto nell'Agenzia.

La posta in partenza viene consegnata all'Ufficio preposto alle operazioni di affrancatura e spedizione, secondo orari prestabiliti.

Eventuali situazioni di urgenza che modifichino la procedura descritta devono essere valutate e autorizzate dalla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi. I corrispondenti destinatari dell'Agenzia sono descritti in appositi elenchi dell'applicativo informatico, costituenti l'anagrafica dell'Agenzia.

10.2 SPEDIZIONE DEI DOCUMENTI INFORMATICI

La spedizione dei documenti informatici avviene all'interno del sistema informatico di gestione dei documenti, dopo essere stati classificati, fascicolati e protocollati, e comunque secondo i seguenti criteri generali:

- i documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari abilitato alla ricezione della posta per via telematica;
- per la spedizione, l'Agenzia si avvale delle caselle di posta elettronica istituzionali, della casella di posta elettronica certificata istituzionale, nonché dei servizi di autenticazione e marcatura temporale offerti da un certificatore abilitato (art. 27, comma 3, DPR 445/00 ed artt. 27 e 28 del CAD);
- gli uffici utente abilitati alla protocollazione provvedono ad effettuare l'invio tramite posta elettronica certificata utilizzando i servizi di autenticazione e marcatura temporale, a verificare l'avvenuto recapito dei documenti spediti per via telematica e ad archiviare le ricevute elettroniche collegandole alle registrazioni di protocollo.

Per la riservatezza delle informazioni contenute nei documenti elettronici, gli addetti alla spedizione si attengono a quanto prescritto dall'art. 49 del CAD.

Per quanto riguarda l'uso della posta elettronica, si rimanda alla precedente Sezione 7 - *“Gestione della posta elettronica”*.

La spedizione di documenti informatici al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni, senza che a queste l'Agenzia riconosca un carattere giuridico-amministrativo che la impegni verso terzi.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

11. SCANSIONE DEI DOCUMENTI CARTACEI

11.1 DOCUMENTI SOGGETTI A SCANSIONE

I documenti su supporto cartaceo soggetti a registrazione di protocollo, di formato inferiore o uguale all'A4, dopo le operazioni di registrazione, classificazione e segnatura, possono essere acquisiti in formato immagine con l'ausilio di *scanner* nel formato conforme alla tecnologia in uso.

11.2 PROCESSO DI SCANSIONE

Il processo di scansione si articola nelle seguenti fasi:

- acquisizione delle immagini in modo che ad ogni documento, anche composto da più fogli, corrisponda un unico file in un formato standard idoneo alla conservazione;
- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- collegamento delle rispettive immagini alla registrazione di protocollo, in modo non modificabile;
- memorizzazione delle immagini, in modo non modificabile;
- il processo di scansione dei documenti cartacei, al fine di trasformarli in formato immagine, avviene nella fase di registrazione del protocollo, a cura dell'ufficio protocollante, anche con attività successive alla registrazione stessa e comunque entro le 48 ore;
- l'unitarietà è garantita dal sistema mediante l'indice di classificazione.

Nel caso in cui si intenda procedere alla scansione sostitutiva dei documenti analogici, oltre alle fasi precedenti, si dovrà procedere alla autenticazione, attraverso sottoscrizione digitale del *file* o di un insieme di *file*, secondo la normativa vigente, come descritto al precedente punto 3.5.

Per quanto riguarda la conservazione dei documenti cartacei scansionati si rimanda al Titolare e al Massimario di scarto (All.1) e al Piano di Conservazione (All.3).

12. CONSERVAZIONE DEI DOCUMENTI

12.1 STRUTTURA DELL'ARCHIVIO

Tutti i documenti prodotti dall'Agenzia costituiscono l'archivio dell'ACSS. In quanto beni culturali, essi devono essere conservati ai sensi della normativa vigente e come tali sono soggetti alla vigilanza della Soprintendenza Archivistica competente per territorio, la quale in tale ambito svolge anche funzioni di consulenza tecnica.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

L'archivio dell'ACSS è suddiviso funzionalmente in archivio corrente, archivio di deposito e archivio storico.

Per Archivio corrente si intende il complesso dei documenti e dei fascicoli relativi a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse corrente. Ne fanno parte anche le banche dati, i sistemi informativi o altri repertori informatizzati che acquisiscono, trattano e conservano dati e informazioni utilizzati ai fini dello svolgimento dell'attività amministrativa. Di norma, per necessità pratiche, i documenti che compongono l'archivio corrente vengono conservati in locali facilmente accessibili o nella stessa stanza del personale che li utilizza.

Per Archivio di deposito si intende il complesso dei documenti, prodotti o ricevuti dall'Agenzia, relativi a pratiche concluse nell'ultimo quarantennio che non servono per l'espletamento delle pratiche correnti, o comunque verso i quali sussiste un interesse sporadico.

Si tratta di una fase intermedia del ciclo di vita di tutti quei documenti che in futuro potrebbero essere scartati, ma che per il momento occorre conservare perché possono ancora essere utili (ad esempio per accertamenti o consultazioni, anche da parte di terzi, nel rispetto dei presupposti e procedure di normative e regolamenti di riferimento).

Presso l'archivio di deposito vengono inoltre trasferiti tutti i documenti per i quali vige l'obbligo di conservazione illimitata.

Per Archivio storico si intende il complesso dei documenti relativi a procedimenti amministrativi e atti conclusi da oltre 40 anni e destinati, previa effettuazione delle operazioni di scarto, alla conservazione permanente per finalità storiche, culturali e di ricerca. Tutta la documentazione anteriore al 1975 costituisce archivio storico.

12.2 PIANO DI CONSERVAZIONE DEI DOCUMENTI

Il Piano di Conservazione (vedi All.3) dell'archivio comprende il Titolario di classificazione e il Massimario di scarto di Regione Lombardia (All.1).

Il suo aggiornamento compete alla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi, in accordo con il Responsabile della Conservazione dei documenti informatici.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

12.3 MEMORIZZAZIONE DEI DOCUMENTI ANALOGICI, DEI DOCUMENTI INFORMATICI E DELLE RAPPRESENTAZIONI DIGITALI DEI DOCUMENTI CARTACEI

I documenti dell'Agenzia sono conservati a cura della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi e del Responsabile della Conservazione dei documenti informatici.

La documentazione corrente è conservata a cura del Responsabile del procedimento, fino al trasferimento in Archivio di deposito.

I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo, e conservati nell'archivio informatico a cura del Responsabile della Conservazione dei documenti informatici.

Le rappresentazioni digitali dei documenti originali su supporto cartaceo, acquisite con l'ausilio dello *scanner*, sono memorizzate nel sistema, in modo non modificabile, al termine del processo di scansione.

12.4 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Il Responsabile della Conservazione dei documenti informatici, d'intesa con il Responsabile del Trattamento dei Dati e con la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi, provvede, in collaborazione con l'ufficio dell'Agenzia preposto alla gestione informatica e con il supporto della tecnologia disponibile:

- a conservare i documenti informatici;
- a controllare periodicamente a campione (almeno ogni sei mesi) la leggibilità dei documenti stessi;
- a salvaguardare gli strumenti di descrizione, ricerca, gestione e conservazione dei documenti.

Va in ogni caso garantita la conservazione integrata dei documenti e delle informazioni di contesto generale, prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi.

I requisiti e le modalità per la conservazione dei documenti informatici sono descritti nel Titolario e Massimario di scarto (All.1), il Piano di Conservazione (All.3) e il Regolamento per la Politica della Sicurezza delle Informazioni e la Cyber Security di ACSS (All.6).

Il sistema deve inoltre fornire la documentazione del software di gestione e conservazione, del sistema di sicurezza, delle responsabilità previste per tutte le fasi di gestione del sistema documentario, delle operazioni di conservazione dei documenti.

La documentazione prodotta nell'ambito del Manuale di gestione e dei relativi aggiornamenti deve essere conservata integralmente e perennemente nell'Archivio dell'Agenzia.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

12.5 CENSIMENTO DEI DEPOSITI DOCUMENTARI, DELLE BANCHE DATI E DEI SOFTWARE

Ogni anno la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi e il Responsabile della Conservazione dei documenti informatici provvedono, ciascuno per la parte di competenza, ad effettuare il censimento dei depositi documentari, dei registri particolari, delle banche dati e dei *software* di gestione documentale in uso all'Agenzia, per programmare i versamenti dei documenti cartacei all'Archivio di deposito, dei documenti informatici su idonei supporti di memorizzazione e per predisporre, di concerto con l'ufficio dell'Agenzia preposto alla gestione informatica, il Piano per la continuità operativa, il *disaster recovery*.

13. GESTIONE DELL'ARCHIVIO

13.1 GLI ARCHIVI CORRENTI

Gli archivi correnti si compongono di documenti prodotti durante lo svolgimento dell'attività amministrativa di cui ai precedenti articoli e sono quelli attualmente in uso e in continuo accrescimento presso le strutture dell'ACSS. L'archivio, quale patrimonio pubblico, non può essere smembrato, a qualsiasi titolo, e deve essere conservato nella sua organicità.

All'interno dei fascicoli correnti i documenti dovrebbero essere posti in ordine cronologico; pertanto, aprendo il fascicolo, si troverà il documento più recente (in entrata e/o in uscita) e poi quello con data antecedente. Questo ordine permette di sapere con certezza cosa, sino a quel momento, è stato svolto o quanto è ancora da realizzare per concludere il procedimento.

13.2 DALL'ARCHIVIO CORRENTE ALL'ARCHIVIO DI DEPOSITO: IL COSIDDETTO SCARTO IN ITINERE

Prima di procedere al trasferimento dei fascicoli dall'archivio corrente all'archivio di deposito, la Struttura dell'Agenzia che ha in carico i fascicoli deve procedere ad una operazione di selezione della documentazione da trasferire, cosiddetta operazione di “scarto in itinere”. In questa fase si deve provvedere ad ordinare i fascicoli secondo la data di formazione del documento ed estrarre dal fascicolo le copie dei documenti ed eventuali minute, appunti, bozze etc., ossia tutto il materiale cartaceo che non costituisce il vero e proprio documento oggetto di conservazione, e che deve essere eliminato.

I documenti devono essere archiviati togliendo eventuali elastici, fermagli, cartellette di plastica, faldoni di plastica o contenenti pezzi di metallo, perché l'umidità, il calore, gli sbalzi di temperatura in genere, con il tempo seccano gli elastici rendendoli inutilizzabili ed arrugginiscono i fermagli. È altresì da evitare lo scotch che con il passare del tempo ingiallisce e si stacca, separando

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

inesorabilmente le parti in precedenza unite. È consigliabile raccogliere tutti i documenti in un involucri cartaceo.

13.3 DOCUMENTAZIONE ELIMINABILE DURANTE LO SCARTO IN ITINERE

Tutti i documenti totalmente superflui ai bisogni ordinari dell'ACSS e **senza validità giuridica** che non hanno necessità di essere conservati in archivi, indipendentemente dal tipo di supporto (analogico/digitale), possono essere eliminati senza autorizzazione della **Soprintendenza Archivistica**. Essi sono, a titolo esemplificativo e non esaustivo, identificabili in:

- minute/appunti/bozze;
- copie e/o fotocopie della corrispondenza e di atti dell'Agenzia;
- copie di file/documenti su supporto informatico/digitale normalmente detenute dalle strutture per uso proprio e/o per comodità di consultazione;
- corrispondenza riservata personale;
- copie delle Gazzette Ufficiali, Bollettini ufficiali della P.A.;
- materiali statistici, libri, giornali, riviste, stampe, periodici, pubblicazioni in genere;
- materiali pubblicitari in genere anche relativi a corsi, convegni e congressi;
- programmi, inviti a manifestazioni che non attivino procedimenti amministrativi;
- modulistica non più in uso e non compilata;
- altra documentazione senza validità giuridica.

Ciascuna Struttura provvede a redigere, al bisogno, una richiesta di ritiro dei materiali da eliminare **senza autorizzazione della Soprintendenza Archivistica**, che contiene le seguenti indicazioni:

- struttura richiedente
- numero dei cartoni/imballi da ritirare;
- ubicazione del materiale
- eventuale presenza di dati sensibili.

La richiesta, autorizzata dal Direttore/Responsabile della Struttura richiedente, deve essere inviata alla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi. Sarà cura della predetta Struttura concordare la data del ritiro con la Struttura richiedente e valutare congiuntamente la modalità di distruzione più opportuna. La Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi resta a disposizione per un eventuale supporto nel processo di valutazione delle modalità di distruzione.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Nella suindicata fase di distruzione di documenti contenenti dati personali e sensibili è garantito il rispetto delle norme in materia di privacy.

13.4 L'ARCHIVIO DI DEPOSITO

Un efficiente archivio di deposito raccoglie, ordina, conserva e rende consultabile tutta la documentazione prodotta e ricevuta dall'Agenzia; pertanto, si presuppone che i fascicoli siano organizzati fin dall'origine, secondo il sistema di classificazione, in modo tale da permettere una agevole identificazione dei documenti ed un facile reperimento degli stessi qualora se ne ravvisi la necessità.

Un efficiente gestione dell'archivio di deposito permette di:

- mantenere il controllo “giuridico” sui documenti per esigenze di natura operativa;
- garantire la reperibilità dei documenti in tempi brevi;
- garantire il rispetto del modello originario di sedimentazione dei documenti.

L'organizzazione dell'archivio di deposito deve consentire la consultazione e l'eventuale recupero immediato di qualsiasi documento necessario per lo svolgimento di pratiche correnti. A tale scopo la sua organizzazione deve rispecchiare, necessariamente, la struttura dell'archivio corrente.

Le funzioni di raccolta, ordinamento, buona conservazione e consultazione della documentazione dell'archivio di deposito, nonché la sicurezza dei documenti medesimi, sono garantite attraverso:

- una corretta gestione della documentazione in ambienti idonei¹ ;
- personale adeguatamente formato;
- ricognizioni periodiche sullo stato di ordinamento e ubicazione della documentazione;
- organizzazione e descrizione del materiale che ne consenta un facile e rapido reperimento;
- l'attività di selezione e di scarto di cui al successivo art. 13.5, al fine di sistemare la documentazione a conservazione permanente per motivi istituzionali, amministrativi o storici

¹ La sede di conservazione archivistica deve innanzitutto essere collocata in un'area priva di rischi. Sono pertanto da evitare collocazioni insistenti o prossime ad aree di esondazione, fiumi, torrenti, canali, frane, prossime a sedi industriali o manifatturiere potenzialmente pericolose (centrali elettriche, raffinerie, industrie chimiche) o a magazzini e depositi in cui sia conservato materiale pericoloso (autorimesse, depositi di detersivi e sostanze infiammabili, depositi di materiale plastico ecc.);

· pareti, pavimenti e soffitti devono essere tali da consentire la massima pulizia del locale ed impedire la proliferazione di parassiti o muffe, nonché scongiurare rischi d'incendio;

· ampie o brusche variazioni dell'umidità o della temperatura dei locali di conservazione sono particolarmente pericolose per la documentazione, poiché danneggiano le fibre della carta e nel contempo favoriscono lo sviluppo e la proliferazione di muffe. I valori indicativi, ottimali per la conservazione di materiale cartaceo, sono di circa 15-18 gradi centigradi di temperatura e 50-60% di umidità relativa. È fondamentale inoltre garantire un adeguato ricambio d'aria, naturale o forzato, al fine di evitare il ristagno di sostanze potenzialmente nocive e la formazione di un microclima favorevole alle muffe e ai parassiti;

· l'eccessiva esposizione al sole e alla luce in genere è di per sé un importante fattore di degrado dei documenti d'archivio; sarebbe dunque opportuno mantenere i depositi al buio o comunque non superare un'illuminazione normale di 50 lux;

· i locali devono disporre di opportuni dispositivi per la sicurezza della documentazione, sia per prevenire il rischio di incendio sia per evitare furti e intrusioni.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

nel contesto dell'archivio storico.

Ciascuna Struttura potrà far confluire nell'archivio di deposito la documentazione relativa a procedimenti esauriti o che abbiano scarsa/sporadica probabilità di consultazione dopo aver effettuato le operazioni di scarto di cui all'art. 13.2.

Le pratiche da trasferire devono essere, per quanto possibile, compatte, evitando in tale modo di archiviare in contenitori di grandi dimensioni un numero esiguo di documenti e procedendo eventualmente all'accorpamento di questi ultimi in un unico contenitore.

Su ogni contenitore occorre applicare l'etichetta (Modulo cod. Pr.04_Mod.02 Rev. 01 “Modello etichetta per contenitori da trasferire presso l'Archivio di deposito”) che identifichi chiaramente l'Agenzia, l'ufficio produttore, la classificazione, l'anno di produzione e la descrizione del contenuto, l'anno di scarto o la dicitura “Conservazione illimitata” se si tratta di documentazione a conservazione perenne.

Per facilitare altresì l'utilizzo di scritte appropriate rispetto al contenuto di ogni contenitore, è indispensabile tenere a riferimento il “Titolario di Classificazione e Massimario di Scarto della documentazione del sistema Sanitario e Socio Sanitario di Regione Lombardia” vigente, quale sistema di classificazione omogeneo, ad applicazione regionale, per tutti gli atti e i documenti delle aziende sanitarie.

Il Titolario è costituito da tre titoli cui corrispondono le tre aree costitutive delle aziende sanitarie: area amministrativa (Titolo 1), area sanitaria e socio-sanitaria territoriale (Titolo 2), area ospedaliera (Titolo 3).

Inoltre:

- ogni titolo è ordinato in classi che evidenziano grandi ambiti di riferimento, ogni classe è articolata in sottoclassi che rappresentano il processo di produzione dell'Agenzia, a prescindere dalla realtà organizzativa nel quale si sviluppa;
- ogni singola voce è accompagnata da un elenco di tipologie documentarie che ne specificano il contenuto.

Durante le operazioni di inserimento dei documenti nei contenitori, si deve procedere per categorie omogenee, inserendo negli stessi le pratiche con la medesima scadenza. La commistione di documenti con scadenze diverse o documenti “a scadenza” con documenti “a conservazione illimitata” renderebbe difficoltosa se non impossibile l'eventuale successiva operazione di scarto.

Su ogni unità di imballaggio deve essere applicata un'etichetta che ne descriva dettagliatamente gli estremi, il contenuto, le date estreme di riferimento e se si tratta di dati sensibili o meno (Modulo

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

cod. Pr.04_Mod.02 Rev. 01 “Modello etichetta per contenitori da trasferire presso l’Archivio di deposito”).

Solo al termine delle sopra riportate operazioni di preparazione e classificazione del materiale, il Responsabile/Direttore della Struttura può procedere ad autorizzare il versamento del materiale identificato presso l’archivio di deposito.

Sarebbe consigliabile non trasferire presso l’archivio di deposito la documentazione soggetta a tempi minimi di conservazione obbligatoria pari a 1 anno, ma di conservarla, piuttosto, presso l’archivio corrente fino alla maturazione del tempo di scarto.

Sarebbe altresì consigliabile che ciascuna Struttura tenesse un elenco dettagliato della documentazione trasferita presso l’archivio di deposito.

Per il trasferimento dei documenti presso il locale dell’Agenzia adibito ad archivio di deposito, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi programma annualmente il versamento dall’archivio corrente a quello di deposito di fascicoli relativi a procedimenti conclusi, coinvolgendo le singole Strutture dell’Agenzia, per la parte di loro competenza, nell’individuazione della documentazione da fare convergere presso il deposito autorizzato dell’ACSS e successivo trasferimento. Tutte le attività connesse al recupero e trasferimento della documentazione vengono coordinate dalla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi.

L’Archivio di Deposito dell’Agenzia censito alla data di redazione della presente procedura operativa è situato nella sede legale dell’Ente in via Pola 12, Milano.

13.5 DALL’ARCHIVIO DI DEPOSITO ALL’ARCHIVIO STORICO: LO SCARTO

Lo scarto rappresenta lo strumento per gestire in maniera ordinata un archivio, permettendo di conservare solo quel che mantiene un rilievo giuridico o ha assunto valore storico.

L’individuazione del materiale documentario da scartare è un’operazione delicata e deve essere effettuata sulla base delle indicazioni contenute nel Titolario e Massimario di scarto vigente.

Gli Archivi degli Enti pubblici appartengono infatti, come già anticipato in premessa, secondo quanto stabilito dal “Codice dei beni culturali” (D.Lgs n.42/2004), al Patrimonio culturale nazionale (artt. 2 e 10). Secondo tale norma, gli archivi e i documenti pubblici sono sempre da considerarsi beni culturali, indipendentemente dalla loro età, tipologia o contenuto, dunque, tutti i documenti prodotti, ricevuti o conservati a qualsiasi titolo da una Pubblica Amministrazione sono beni culturali. Pertanto, non è assolutamente consentito il semplice “mandare al macero i documenti quando non servono più”.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Tutti i documenti per i quali sono stati superati i tempi di conservazione previsti dal Massimario di scarto dovranno essere sottoposti alla procedura di scarto di seguito indicata.

La valutazione circa la possibilità di scarto della documentazione dovrà essere effettuata dal Responsabile della Struttura proponente in relazione a quanto stabilito dal predetto Titolare e Massimario di scarto.

13.6 PREDISPOSIZIONE DELLA DOCUMENTAZIONE

Dalla documentazione selezionata, se non già fatto in precedenza come dà indicazioni di cui al sopra richiamato Art. 13.4, occorre eliminare tutto quello che non è semplicemente di carta, ossia: raccoglitori di plastica, buste di plastica, fermagli, elastici ecc.; tale documentazione deve essere raccolta in cartoni, scatole, cartelle o altri imballaggi idonei per tipologie omogenee (anche in riferimento all'anno di scadenza) che devono essere sottoposti a pesatura. Le scatole dovranno essere opportunamente sigillate, a tutela dei dati personali, sensibili in esse contenuti. Su ogni unità di imballaggio – se non effettuato al momento del versamento in archivio di deposito – deve essere applicata un'etichetta che ne descriva dettagliatamente gli estremi, il contenuto, le date estreme di riferimento e se si tratta di dati sensibili o meno (Modulo cod. Pr.04_Mod.02 Rev. 01 “Modello etichetta per contenitori da trasferire presso l'Archivio di deposito”).

13.7 COMPILAZIONE ELENCO DOCUMENTAZIONE PER LO SCARTO

Ciascuna Struttura, per quanto di propria competenza, provvede a redigere la proposta di scarto utilizzando il modulo allegato (Modulo cod. Pr.04_Mod.01 Rev. 01 “Modello per gli atti da proporre allo scarto”), che contiene le seguenti indicazioni:

- classificazione della documentazione come da Titolare e Massimario di scarto;
- descrizione degli atti: per la tipologia dei documenti occorre fare riferimento alla descrizione della voce riportata nel Massimario di scarto approvato da Regione Lombardia in vigore (anche per affinità): es...;
- date estreme dei documenti;
- tipologia e quantitativo dei contenitori: cartelle, pacchi, sacchi, registri, fascicoli, cartoni, ecc.;
- peso presunto della documentazione stimato in kg. Il peso può essere così stimato: 1 metro lineare = mediamente 50 kg; 1 m³ = mediamente 600 kg;
- eventuali osservazioni.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

L'elenco deve essere firmato e timbrato dal Direttore/Responsabile della Struttura proponente lo scarto, come garante della corrispondenza tra l'elenco del materiale di cui si chiede l'autorizzazione allo scarto e la documentazione raccolta e imballata a tale scopo.

La proposta di scarto deve essere inviata alla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Terminate le operazioni di verifica della congruità della richiesta rispetto al vigente Massimario di scarto, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi invia la richiesta di autorizzazione allo scarto alla Soprintendenza Archivistica per la Lombardia, ai sensi dell'articolo 21, lett. d) del Codice per i beni culturali.

Ottenuto il nulla osta da parte della suddetta Soprintendenza, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi lo trasmette alla Struttura richiedente, con la quale provvederà a pianificare il ritiro del materiale oggetto di scarto. Sarà responsabilità della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi contattare il fornitore dei servizi di ritiro, trasporto e smaltimento della documentazione cartacea per i successivi adempimenti.

Terminato il processo di distruzione, il fornitore restituisce il verbale di avvenuta distruzione alla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi, che lo inoltra alla Struttura richiedente.

Per il completamento della procedura, la Struttura richiedente procede a trasmettere alla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi copia del “verbale di distruzione” della documentazione, sul quale dovranno essere riportati il numero degli imballaggi e il peso della documentazione scartata, richiamando nella trasmissione del succitato attestato il numero di riferimento pratica, indicato sul nullaosta.

Ad esito della procedura di scarto, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi trasmette alla Soprintendenza archivistica l'attestazione dell'avvenuta distruzione.

In tutte le fasi dello scarto di documenti contenenti dati personali e sensibili è indispensabile garantire il rispetto delle norme in materia di privacy.

13.8 FREQUENZA DELLE OPERAZIONI DI SCARTO

La Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi programma con cadenza annuale il processo di scarto. La calendarizzazione delle operazioni

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

di cui trattasi è volta a impostare una metodologia che garantisca una periodica individuazione della documentazione per la quale sono superati i tempi di conservazione e successivo smaltimento. Entro il mese di marzo di ogni anno le Strutture saranno invitate a individuare e quantificare il materiale documentale oggetto di smaltimento e redigere una proposta di scarto.

13.9 RESPONSABILITÀ SULL'OSSERVANZA DELLE NORME SULLO SMALTIMENTO

Almeno una volta l'anno, in base al Massimario di scarto viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale, a cura della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi con l'invio della proposta alla Soprintendenza Archivistica per la Lombardia.

Lo scarto di documenti dell'archivio dell'Ente è quindi subordinato ad autorizzazione della Soprintendenza Archivistica. È fatto quindi divieto assoluto di scarto/distruzione di materiale soggetto a conservazione senza averne preventivamente acquisito il nullaosta.

La distruzione non autorizzata di documenti dell'archivio è punita con l'arresto da sei mesi a un anno e con l'ammenda da euro 775 ad euro 38.734,50 (art. 169, c.1-a D.Lgs 42/2004).

L'autorizzazione della Soprintendenza non sana l'illegittimità di eventuali scarti prematuri di documentazione che, pur non essendo destinata alla conservazione permanente, ha una sua temporanea validità giuridica o utilità funzionale ed economica.

13.10 L'ARCHIVIO STORICO

L'archivio storico rappresenta la terza e ultima fase di vita dell'archivio dell'Agenzia; in questa fase lo scarto è vietato.

L'archivio storico svolge funzioni di conservazione, ordinamento, inventariazione del patrimonio documentario assicurandone la consultabilità, ed è costituito dai documenti relativi agli atti ed ai procedimenti esauriti da oltre quarant'anni.

I documenti ed i fascicoli selezionati per la conservazione permanente devono essere ordinati rispettando i criteri delineati per l'archiviazione corrente e di deposito.

L'archivio storico deve essere correttamente conservato, è inalienabile ed è sottoposto alla vigilanza della Soprintendenza competente per territorio.

L'archivio storico deve inoltre essere inventariato, cioè, dotato di uno strumento di descrizione complessiva che, affiancando gli strumenti originari di gestione (protocolli, repertori, ecc.), ne facilita

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

l'accesso ai fini giuridico-amministrativi e di ricerca scientifica, e ne consenta la tutela anche patrimoniale.

La sua gestione deve sempre e comunque garantire autenticità, integrità e reperibilità di tutti i documenti in esso contenuti.

Ai sensi dell'art. 122 del Codice per i beni culturali e del paesaggio, gli archivi storici per la tenuta della documentazione amministrativa, sono liberamente consultabili salvi i limiti di riservatezza previsti dalla normativa in materia di protezione dei dati personali.

L'ambiente dedicato alla consultazione dei documenti dovrà sempre essere separato dall'ambiente destinato alla conservazione ed entrambi i locali dovranno consentire un agevole controllo da parte del personale incaricato della vigilanza.

13.11 PERIODI MINIMI DI CONSERVAZIONE

Il Massimario di scarto è il documento che permette di gestire correttamente il ciclo di vita dei documenti. Il Massimario consiste in un elenco ragionato di tipi di documenti di cui si compone l'archivio (categorie del Titolare) in cui vengono indicati, per ciascuno di essi, i periodi minimi di conservazione obbligatoria dopo i quali si può procedere alla loro eliminazione.

Grazie a questo strumento, l'archivio non verrà aggravato da documentazione non utile ai fini per i quali è stato creato.

È indispensabile precisare che è demandata alla responsabilità dei Direttori/Responsabili di ciascuna Struttura coinvolta l'eventuale decisione sull'estensione del lasso temporale - al di là di quanto astrattamente previsto, in linea generale, dal Titolare di Classificazione e Massimario di Scarto (All.1) - di mantenimento di alcune tipologie di documenti per ogni utilità amministrativa, contabile o legale del documento stesso.

13.12 DOCUMENTAZIONE A CONSERVAZIONE ILLIMITATA

Tra i documenti a conservazione perenne, si citano, a mero titolo esemplificativo:

- atti di carattere normativo e regolamentare interno ed esterno all'Agenzia (delibere, ordinanze, determinazioni, circolari);
- attestazioni di natura patrimoniale (inventari,);
- documenti contabili di sintesi (bilanci e conti consuntivi, libri mastri, giornali di cassa);
- documenti contabili (fatture elettroniche e relative notifiche);
- documenti giudiziari (sentenze, atti relativi al contenzioso);
- atti riguardanti il personale (fascicoli del personale, libri matricola);
- atti che caratterizzano l'attività dell'Agenzia (atti istituzionali e specifici dell'Agenzia).

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

13.13 RESPONSABILITÀ SULLA TENUTA DEGLI ARCHIVI

Sulla corretta tenuta e conservazione degli archivi dell'Agenzia si rimanda a quanto stabilito al paragrafo 2.2.

14. PUBBLICITA' LEGALE E TRASPARENZA AMMINISTRATIVA

14.1 MODELLI PUBBLICATI

L'Agenzia rende disponibile per via telematica l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà. I modelli di documenti pubblicati sul sito internet o sulla rete intranet sono classificati secondo il piano di classificazione in uso.

14.2 OBBLIGHI DI PUBBLICITÀ TRASPARENZA E DIFFUSIONE DI INFORMAZIONI

La trasparenza, ai sensi della Legge sulla trasparenza amministrativa, è intesa come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività dell'Agenzia, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche. La trasparenza, nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio, di segreto statistico e di protezione dei dati personali, concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione. Essa è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali e concorre alla realizzazione di un'amministrazione aperta, al servizio del cittadino. Nel Piano Integrato di Attività e Organizzazione 2024-2026 (PIAO) dell'Agenzia, approvato con Deliberazione n. 1 del 17/01/2024 e s.m.i. con Deliberazione n. 2 del 21/02/2024, sono allegati la Griglia degli obblighi di pubblicazione ex D.Lgs. n.33/2013, indicante gli ambiti di pertinenza di ACSS, e la Procedura di pubblicazione in AT dei medesimi; in presenza di modifiche al PIAO di tali previsioni, si dovrà riferire ai contenuti della griglia e delle procedure come previsti alla corrispondente nuova previsione del PIAO vigente e alle sue successive modifiche e integrazioni.

14.3 ATTUAZIONE DEL GDPR: GESTIONE DEI DATI

In data 25/05/2018 è divenuto operativo il nuovo Regolamento UE 2016/679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, al quale si affianca la disciplina prevista dal D. Lgs. 196 del 30/06/2003

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

(Codice Privacy), modificata dal D.Lgs. n.101 del 10/08/2018 “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679”. Particolare attenzione viene riservata dal Garante Privacy alla correlazione che sussiste tra trasparenza e tutela dei dati personali, risolta nei termini di un “bilanciamento” tra diritto alla riservatezza (inteso come diritto a controllare la circolazione delle informazioni riferite alla propria persona) e diritto dei cittadini al libero accesso ai dati, alle informazioni e ai documenti per i quali è prevista la pubblicazione obbligatoria in AT (accesso civico) ovvero la messa a disposizione ove detenuti dalla PA (accesso generalizzato - FOIA). L'Agenzia, con Deliberazione n. 9 del 21/12/2022, ha approvato il “Regolamento sul trattamento dei dati personali di ACSS” che, oltre a tracciare i passaggi fondamentali per la gestione delle richieste di accesso ai dati, fornisce indicazioni di carattere organizzativo per l'individuazione degli uffici competenti a decidere sulle istanze, le modalità e i tempi per lo svolgimento dell'istruttoria procedurale e per le comunicazioni con il cittadino, specificando i casi di esclusione e di limitazione di accesso in conformità con l'ordinamento giuridico. L'Agenzia, anche con riferimento agli adempimenti connessi alla trasparenza in attuazione del D.Lgs. n. 33/2013, come modificato dal D.Lgs. n. 97/2016 e agli ulteriori atti emanati da ANAC (linee guida, delibere, atti del presidente ANAC ecc...), agisce nel rispetto del regime privacy: la pubblicazione dei dati e dei documenti (in generale sul sito web istituzionale incluso l'Albo Pretorio e in particolare nella sezione AT) viene effettuata nel rispetto dei principi applicabili al trattamento dei dati personali contenuti nell'art. 5 del Regolamento UE 2016/679 (liceità, correttezza e trasparenza, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza), nonché del principio di responsabilizzazione (accountability), in questa sede interpretato come impegno a “dare conto” delle attività e delle azioni poste in essere

15. ACCESSO

15.1 ACCESSIBILITÀ AL SISTEMA DI PROTOCOLLO E LIVELLI DI RISERVATEZZA

La riservatezza delle registrazioni di protocollo o di altri registri e dei documenti informatici è garantita dal sistema attraverso l'uso di profili personali e *password* (o altre tecniche e dispositivi di autenticazione sicura). L'operatore che effettua la registrazione di protocollo inserisce il livello di riservatezza richiesto per il documento in esame, altrimenti il sistema applica automaticamente l'inserimento di un livello *standard* predeterminato.

In modo analogo, al momento dell'apertura di un nuovo fascicolo deve esserne determinato il livello di riservatezza.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

Il livello di riservatezza applicato a un fascicolo si estende a tutti i documenti che ne fanno parte. In particolare, un documento con livello minore di quello del fascicolo assume il livello del fascicolo di inserimento, mentre mantiene l'eventuale livello maggiore.

In attuazione della legge n. 241/90 e ss.mm. e ii., del D.P.R. 12 aprile 2006, n. 184, del D.Lgs. n. 42/2004 e ss.mm. e ii., e tenuto anche conto di quanto contenuto nel D.Lgs. del 30 giugno 2003, n. 196, nonché al GDPR, l'Agenzia ha approvato con Deliberazione n. 7 del 21/09/2022, il proprio *“Regolamento per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico semplice e generalizzato (All.5)”*, consultabile anche sul Sito Internet dell'Agenzia (all'indirizzo: Accesso civico - www.acsslombardia.it). I RPCT, in collaborazione con la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi, in conformità alla normativa di riferimento, redige in formato digitale il “Registro degli Accessi” recante l'elenco delle richieste di accesso pervenute e ne assicura l'aggiornamento semestrale e la pubblicazione nella sezione amministrazione trasparente del sito web istituzionale, come specificato nel “Piano Integrato di attività e organizzazione 2024-2026 (PIAO)”. Per ciascuna istanza viene indicato l'oggetto e la data della richiesta, nonché il relativo esito con la data della decisione.

Ai sensi dell'art. 72 e ss. del CAD, l'accesso al sistema informatico documentale da parte di pubbliche amministrazioni è realizzato applicando le norme ed i criteri tecnici emanati per la realizzazione del Sistema Pubblico di Connettività (SPC) o sulla base di specifiche convenzioni.

16. GESTIONE DELL'EMERGENZA

Le piccole e grandi catastrofi stanno colpendo sempre più spesso il nostro Paese e gli archivi sono particolarmente esposti ai rischi derivanti da diverse calamità: la carta e le pergamene sono infatti molto sensibili ad elementi distruttivi quali il fuoco o l'acqua, nonché ad altri agenti, apparentemente più lenti ma ugualmente nocivi, quali la polvere, l'umidità, le muffe.

La Soprintendenza archivistica e bibliografica della Lombardia ha promosso e coordinato la redazione di un *“Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche – Soprintendenza archivistica e bibliografica della Lombardia”* (All.2), che fornisce linee guida utili a prevenire e affrontare le emergenze in archivio.

L'approccio da adottare non può che essere, in primo luogo, la prevenzione: è indispensabile che l'archivio sia gestito nel modo migliore, così da ridurre al minimo i rischi, che quindi vanno preventivamente conosciuti ed analizzati.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

La prima attività da cui partire è dunque la conoscenza del patrimonio archivistico: sapere dove si trova l'archivio dell'Agenzia (in quale sede e in quali locali), conoscere il rischio legato ai locali che lo custodiscono e prevederne misure di prevenzione.

A mero titolo esemplificativo, considerato il costante aumento di eventi idrogeologici e metereologici estremi, è preferibile evitare la conservazione di materiale cartaceo in locali seminterrati o sotterranei, in quanto facilmente soggetti ad allagamenti e infiltrazioni. Nel caso di archivi siti in locali che si trovano a una quota inferiore (anche solo in parte) a quella del terreno posto in aderenza all'edificio, è bene non riporre materiale negli scaffali più vicini al pavimento, al fine di evitare danni da acqua.

È anche necessario che l'Agenzia e il personale incaricato di gestire l'archivio siano preventivamente preparati a eventuali emergenze, sia con un'adeguata formazione degli operatori (corsi antincendio previsti dalla legge), sia con adeguate attrezzature e strutture ², sia con protocolli di comportamento specifici e adatti alle diverse tipologie di calamità.

16.1 MISURE DA ADOTTARE IN CASO DI EMERGENZA

In caso di emergenza è necessario far intervenire immediatamente, ove il caso lo richieda, gli organi e i corpi preposti alla sicurezza delle persone e delle strutture (Vigili del Fuoco, Protezione Civile, Carabinieri, Polizia).

Contemporaneamente è opportuno avvertire, con la massima sollecitudine, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi e trasmettere alla stessa la Scheda Rilevazione Danni (allegato 1 del sopracitato Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche) debitamente compilata e corredata da documentazione fotografica del bene danneggiato, oltre che da relazione tecnica emessa dal competente Ufficio sullo stato dei locali/immobili colpiti da eventi avversi.

La Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi procede a denunciare l'evento alla Soprintendenza Archivistica, che valuterà i rischi per il materiale tutelato e potrà dettare le corrette procedure di intervento e recupero.

È fatto assoluto divieto di precedere alla rimozione/distruzione del materiale danneggiato senza preventivo intervento e autorizzazione della Soprintendenza.

² La Soprintendenza Archivistica, quale organo periferico del Ministero per i Beni e le Attività Culturali, esercita la vigilanza sulla buona conservazione e la sicurezza degli archivi e dei singoli documenti: essa ha perciò il compito di controllare le sedi in cui gli archivi sono conservati e, ove si accertino situazioni di pericolo o di potenziale rischio per i beni, prescrivere i necessari adeguamenti.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

17. DISPOSIZIONI FINALI

17.1 NORMA DI RINVIO

Per quanto non previsto dalla presente procedura operativa si fa rinvio alla disciplina vigente in materia.

17.2 APPROVAZIONE, INTEGRAZIONI, MODIFICHE ED AGGIORNAMENTI DEL MANUALE

Dalla data di entrata in vigore della presente procedura operativa, sono abrogate tutte le precedenti disposizioni interne dell'Agenzia di Controllo del Sistema Socio Sanitario Lombardo (ACSS) relative alla materia ivi trattata.

Il presente Manuale è approvato, integrato e modificato con Decreto del Direttore Generale dell'Agenzia.

Il presente Manuale è soggetto a revisione ordinariamente, ogni due anni, su iniziativa della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi. La modifica o l'aggiornamento di uno o di tutti i documenti allegati al presente Manuale non comporta la revisione del Manuale stesso.

Qualora se ne presenti la necessità si potrà procedere a revisione del Manuale anche prima della scadenza prevista a cura della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Il presente Manuale è stato trasmesso alla Soprintendenza Archivistica per la Lombardia che ne ha approvato il testo.

17.3 PUBBLICAZIONE DEL MANUALE

Il Manuale di gestione è reso pubblico tramite la sua pubblicazione sul sito internet dell'amministrazione, in un'apposita sezione dell'area "Amministrazione Trasparente – Atti generali". La pubblicazione viene effettuata nell'albo online degli atti di adozione e revisione e deve essere inviata copia alla Soprintendenza archivistica e ad altri enti o uffici.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

18. RIFERIMENTI NORMATIVI

- **Legge 7 agosto 1990, n. 241 e ss. mm. e ii.** - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
- **Decreto del Presidente della Repubblica 10 novembre 1997, n. 513** - Regolamento contenente i criteri e le modalità di applicazione dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici.
- **Decreto del Presidente della Repubblica 20 ottobre 1998, n. 428** - Regolamento recante norme per la gestione del protocollo informatico da parte delle amministrazioni pubbliche.
- **Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999** - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513.
- **Direttiva del Presidente del Consiglio dei Ministri 28 ottobre 1999** - Gestione informatica dei flussi documentali nelle pubbliche amministrazioni.
- **Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000** - Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428.
- **AIPA Deliberazione n. 51/2000 del 23 novembre 2000** - Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513.
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445** - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
- **Decreto legislativo 23 gennaio 2002, n. 10** - Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.
- **Ministro per l'innovazione e le tecnologie - 9 dicembre 2002** - Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.
- **Decreto del Presidente della Repubblica 7 aprile 2003, n. 137** - Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10.

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

- **Decreto legislativo 30 giugno 2003 n. 196** - Codice in materia di protezione dei dati personali.
- **Ministro per l'innovazione e le tecnologie - 14 ottobre 2003** – Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi.
- **Dipartimento per l'innovazione e le tecnologie - Direttiva 27 novembre 2003**- Impiego della posta elettronica nelle pubbliche amministrazioni.
- **Direttiva del Ministero per l'Innovazione e le Tecnologie 19 dicembre 2003** - “Sviluppo ed utilizzazione dei programmi informatici da parte delle pubbliche Amministrazioni.
- **CNIPA Deliberazione 19 febbraio 2004, n.11** - Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.
- **Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004** - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.
- **Decreto Legislativo 22 gennaio 2004 n.42**– Codice dei beni culturali e del paesaggio, ai sensi dell’articolo 10 della legge 6 luglio 2002, n. 137.
- **Decreto legislativo 7 marzo 2005, n.82** - Codice dell'amministrazione digitale (così come modificato e integrato dal **D.Lgs. 30 dicembre 2010, n. 235**)
- **CNIPA Circolare 6 settembre 2005, n.48** - Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
- **Decreto legislativo 4 aprile 2006, n.159** - Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n.82, recante codice dell'amministrazione digitale.
- **Decreto legislativo 24 marzo 2006, n.156** - Disposizioni correttive ed integrative al decreto legislativo 22 gennaio 2004, n.42, in relazione ai beni culturali.
- **Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009** - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.
- **Decreto del Presidente del Consiglio dei Ministri 6 maggio 2009** - Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini.
- **CNIPA - Linee guida per l'utilizzo della firma digitale – Versione 1.3 – Aprile 2009.**

 	PROCEDURA OPERATIVA GENERALE “MANUALE DI GESTIONE DOUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI”	Cod: Pr.04 Rev: 01 Data: 16/06/2025

- **CNIPA Deliberazione 21 maggio 2009, n.45** - Regole per il riconoscimento e la verifica del documento informatico.
- **Agenzia per l'Italia Digitale (AGID) 1° gennaio 2022** - Linee guida sulla formazione, gestione e conservazione dei documenti informatici.
- **Agenzia per l'Italia Digitale (AGID) 21 dicembre 2022:** Linee guida sull' Accessibilità degli strumenti informatici.
- **Titolario e Massimario del Sistema Sociosanitario lombardo** già Sistema Sanitario e Sociosanitario di Regione Lombardia. Revisione 04.

20. DOCUMENTI COLLEGATI

1. Modulo cod. Pr.04_Mod.01 Rev.01 “Modello per gli atti da proporre allo scarto.”
2. Modulo cod. Pr.04_Mod.02 Rev.01 “Modello etichetta per contenitori da trasferire presso l'Archivio di deposito.”

19. ALLEGATI

Allegato n. 1: Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia. Revisione 04.

Allegato n. 2: Piano di conoscenza per la sicurezza di Archivi e Biblioteche - Soprintendenza archivistica e bibliografica della Lombardia.

Allegato n. 3: Piano di conservazione.

Allegato n. 4: Piano di fascicolazione.

Allegato n. 5: Regolamento per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico semplice e generalizzato – ACSS deliberazione n. 07 del 21/09/2022.

Allegato n. 6: Regolamento per la Politica della Sicurezza delle Informazioni e la Cyber Security di ACSS.

Allegato n. 7: Organigramma ACSS.

 	MODULO Modello etichetta per contenitori da trasferire presso l'Archivio di deposito	Cod: Pr.04_Mod.02 Rev. 01 Data:16/06/2025

 
Descrizione struttura
Contenuto e natura dati
Estremi cronologici: dal ____ al ____ Titolario: _____ Classificazione: _____ Sottoclassificazione: _____ N. progressivo _____ di _____ Anno di scarto: _____

Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

Revisione 04

Nel presente Titolario e Massimario di scarto in revisione 04 le modifiche inserite, rispetto alla versione precedente, sono riportate in carattere corsivo.

Titolario di classificazione

Revisione 04

TITOLARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04

Titolo 1 - Area Amministrativa		
Classe	Sottoclasse	Descrizione
1	.00	Amministrazione generale
1	.01	Normativa e provvedimenti
1	.02	Programmazione, disposizioni, indirizzi e obiettivi dell'ente, atti di organizzazione
1	.03	Protocolli di intesa, convenzioni con enti pubblici e privati, no profit
1	.04	Controlli interni ed esterni
1	.05	Sistema Qualità e Risk Management
1	.06	Progetti di ricerca
1	.07	Associazioni di volontariato e di tutela dei diritti del malato
1	.08	Politiche ed interventi per le pari opportunità
2	.00	Organi e organismi
2	.01	Legale Rappresentante
2	.02	Organismi direttivi e scientifici
2	.03	Organismi di controllo interno ed esterno
2	.04	Collegi, Comitati e Commissioni
3	.00	Attività giuridico-legale
3	.01	Pareri, informative giuridiche e attività tecnico-legali
3	.02	Contenzioso legale
3	.03	Procedure concorsuali ed esecutive
3	.04	Assicurazioni e gestione sinistri
4	.00	Risorse umane
4	.01	Dotazione organica e gestione del personale
4	.02	Concorsi e selezioni
4	.03	Assunzioni, inquadramenti, incarichi e cessazioni
4	.04	Istituti contrattuali sospensivi della prestazione lavorativa
4	.05	Organizzazioni sindacali e contrattazione
4	.06	Retribuzione e compensi
4	.07	Trattamenti fiscali, contributivi e assicurativi
4	.08	Inabilità al lavoro, invalidità, infermità, indennizzo
4	.09	Presenze e assenze
4	.10	Quiescenza e relativo trattamento
4	.11	Servizi a richiesta individuale
4	.12	Valutazione del personale
4	.13	Formazione e aggiornamento del personale
4	.14	Deontologia professionale ed etica del lavoro
4	.15	Personale non strutturato o convenzionato
5	.00	Risorse finanziarie e gestione contabile
5	.01	Attività finanziaria e contabile
5	.02	Bilancio e rendicontazione
5	.03	Gestione entrate-uscite
5	.04	Gestione fiscale e imposte
6	.00	Gestione e organizzazione del patrimonio
6	.01	Progettazione e costruzione di beni immobili con relativi impianti
6	.02	Acquisizione e gestione beni immobili e relativi servizi
6	.03	Acquisizione e gestione beni mobili / generi di consumo e di servizi
6	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso
6	.05	Attività contrattuale e tutela della proprietà intellettuale
6	.06	Sicurezza degli ambienti di lavoro
6	.07	Gestione dei rifiuti
7	.00	Sistemi Informativi e comunicazione
7	.01	Sistema documentale
7	.02	Rapporti con il pubblico, sportelli informativi e trasparenza
7	.03	Tutela della riservatezza
7	.04	Biblioteche e centri di documentazione
7	.05	Sistema informatico, reti e sicurezza
7	.06	Statistiche e reporting

TITOLARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04

Titolo 2 - Area Sanitaria e Socio-Sanitaria Territoriale

Classe	Sottoclasse	Descrizione
1	.00	Organizzazione territoriale
1	.01	Gestione e organizzazione dipartimentale e interdipartimentale, distrettuale ed interdistrettuale
1	.02	Progetti, interventi e iniziative varie dipartimentali / distrettuali
1	.03	Coordinamento e gestione personale infermieristico, tecnico-assistenziale, di prevenzione
2	.00	Prevenzione e sicurezza negli ambienti di lavoro
2	.01	Aspetti generali, organizzativi e gestionali
2	.02	Medicina del lavoro e malattie professionali
2	.03	Igiene e sicurezza sul lavoro
2	.04	Sicurezza e impiantistica
3	.00	Prevenzione medico - sanitaria
3	.01	Aspetti generali, organizzativi e gestionali
3	.02	Educazione sanitaria
3	.03	Epidemiologia e profilassi malattie infettive e parassitarie
3	.04	Prevenzione malattie cronico-degenerative
3	.05	Igiene urbana, ambientale e sanità pubblica
3	.06	Tutela salute attività sportive
3	.07	Igiene degli alimenti
3	.08	Igiene della nutrizione
3	.09	Laboratorio di prevenzione
4	.00	Prevenzione veterinaria
4	.01	Aspetti generali, organizzativi e gestionali
4	.02	Sanità animale
4	.03	Anagrafe zootecnica e movimentazione animale
4	.04	Igiene alimenti di origine animale
4	.05	Igiene allevamenti e produzioni zootecniche
4	.06	Randagismo e tutela animali da affezione
5	.00	Assistenza sanitaria
5	.01	Aspetti generali, organizzativi e gestionali
5	.02	Emergenza sanitaria territoriale
5	.03	Assistenza sanitaria di base
5	.04	Assistenza protesica e integrativa
5	.05	Assistenza psichiatrica e neuropsichiatrica infantile
6	.00	Assistenza socio-sanitaria integrata
6	.01	Aspetti generali, organizzativi e gestionali
6	.02	Dipendenze
6	.03	Famiglia, infanzia ed età evolutiva
6	.04	Assistenza domiciliare
6	.05	Disabilità
6	.06	Fragilità
7	.00	Governo sanitario e sociosanitario
7	.01	Aspetti generali, organizzativi e gestionali
7	.02	Osservatorio epidemiologico
7	.03	Flussi informativi sanitari e sociosanitari
7	.04	Accreditamento e controllo strutture sanitarie
7	.05	Autorizzazione e controllo strutture sociosanitarie
7	.06	Acquisto e controllo prestazioni sanitarie
7	.07	Acquisto e controllo prestazioni sociosanitarie
8	.00	Medicina legale
8	.01	Aspetti generali, organizzativi e gestionali
8	.02	Attività medico-legale e necroscopica
8	.03	Invalidità civile, sordomutismo e menomazioni visive
8	.04	Istanze di indennizzo
9	.00	Assistenza e governo farmaceutica
9	.01	Aspetti generali, organizzativi e gestionali
9	.02	Controllo spesa farmaceutica
9	.03	Controllo farmacie, parafarmacie e distributori
9	.04	Autorizzazione e governo farmacie
9	.05	Farmacovigilanza
9	.06	Assistenza farmaceutica diretta
9	.07	Sperimentazione farmaci e dispositivi
9	.08	Gestione stupefacenti

TITOLARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04

Titolo 3 - Area Ospedaliera		
Classe	Sottoclasse	Descrizione
1	.00	Direzione ospedaliera
1	.01	Aspetti generali, organizzativi e gestionali
1	.02	Rapporti con l'autorità giudiziaria
1	.03	Igiene ospedaliera
1	.04	Radioprotezione
2	.00	Pronto soccorso
2	.01	Gestione organizzativa P.S.
2	.02	Attività emergenza-urgenza
3	.00	Assistenza ospedaliera
3	.01	Aspetti generali, organizzativi e gestionali
3	.02	Ricovero (ordinario, day hospital, day surgery)
3	.03	Day service
3	.04	Assistenza al parto
3	.05	Assistenza domiciliare
3	.06	Medicina penitenziaria
3	.07	Assistenza psichiatrica e neuropsichiatrica infantile
4	.00	Assistenza ambulatoriale
4	.01	Prestazioni ambulatoriali
5	.00	Riabilitazione
6	.00	Attività immuno-trasfusionale
6	.01	Aspetti generali, organizzativi e gestionali
6	.02	Valutazione idoneità donatori sangue ed emocomponenti
7	.00	Attività di trapianto d'organi e tessuti
7	.01	Aspetti generali, organizzativi e gestionali
7	.02	Donazione e prelievo
8	.00	Farmaceutica ospedaliera
8	.01	Farmaceutica
8	.02	Stupefacenti
9	.00	Medicina legale ospedaliera
9	.01	Medicina necroscopica
9	.02	Indennizzo danni
9	.03	Consulenze medico-legali
10	.00	Medicina del lavoro
10	.01	Cartella sanitaria e di rischio del lavoratore
10	.02	Malattia professionale e infortunio sul lavoro
11	.00	Sperimentazione clinica dei medicinali e dei dispositivi

Massimario di scarto

Revisione 04

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 1 - Area Amministrativa

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
1. Amministrazione Generale	.01	Normativa e provvedimenti	Normativa e relativa attuazione di carattere generale riferita ad atti esterni (normativa statale, regionale, pareri, circolari, direttive, delibere di altri Enti)	5 anni	
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Registro Deliberazioni / Determinazioni	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali. Deliberazioni (raccolta)
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Atti e provvedimenti emessi dall'Ente <i>originali</i> (Deliberazioni, Determinazioni, <i>corrispondenza di natura istituzionale</i> , ecc.)	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali. Circolari interne esplicative e direttive / Ordinanze
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Regolamenti aziendali e le relative fasi procedurali (dalla proposta all'adozione del testo definitivo)	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali. Circolari interne esplicative e direttive / Ordinanze
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Documento di Programmazione	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Piani Aziendali (Piano dei Controlli, Piano Salute, Strategici, Piano delle Performance, Piano anticorruzione, Modello organizzativo ecc.)	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Disposizioni e comunicazioni a carattere transitorio (<i>convocazioni, inviti, corrispondenza varia, ecc.</i>)	5 anni	
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	RAR, Progetti speciali, obiettivi regionali e aziendali	15 anni	
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Sperimentazioni gestionali	ILLIMITATO	
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Deleghe (di funzioni, attività, di firma) e Funzioni delegate da altri enti (Stato, Regioni, Comuni)	15 anni	
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Piano di organizzazione e funzionamento aziendale (<i>POAS</i> , <i>POFA</i>)	ILLIMITATO	
	.03	Protocolli di intesa, convenzioni con enti pubblici e privati, no profit	Convenzioni / collaborazioni con istituzioni varie (incluse convenzioni di tirocinio e convenzioni per accertamento d'ufficio PA certificanti)	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali
	.04	Controlli interni ed esterni	Documenti relativi ai controlli interni (es. controllo di gestione, contabilità analitica, controllo strategico, auditing, controllo di regolarità formale e contabile, ecc.)	10 anni; ILLIMITATO se allegate a delibere o a documenti di programmazione	
	.04	Controlli interni ed esterni	Documenti relativi ai controlli esterni (es. ispezioni e controlli effettuati da soggetti come la Corte dei Conti, Ministero della Salute, ecc.)	ILLIMITATO	
	.05	Sistema Qualità e Risk Management	Documenti relativi al sistema di gestione per la qualità (Verbal audit ISO, procedure aziendali, certificati ISO, riesame direzione, <i>questionari</i> customer satisfaction, piani qualità, ecc.)	10 anni	
	.05	Sistema Qualità e Risk Management	Scheda di incident reporting, raccolta e analisi dei rischi clinici, incident reporting, analisi statistica di principali sinistri, piano annuale di risk management	ILLIMITATO	
	.06	Progetti di Ricerca	Progetti di ricerca regionali, aziendali, altri progetti	5 anni	
	.07	Associazioni di volontariato e tutela dei diritti del malato	Rapporti con il mondo associativo, del no-profit, di tutela malati, ecc.	ILLIMITATO	
	.08	Politiche e interventi per le pari opportunità	Politiche sulle pari opportunità compresi convegni, congressi, questionari, ecc.	10 anni	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 1 - Area Amministrativa

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
2. Organi e Organismi	.01	Legale Rappresentate	Documenti relativi a Presidente, Direttore Generale o altra figura (nomina, compiti, rinnovo, cessazione e atti inerenti, ecc.)	ILLIMITATO	
	.01	Legale Rappresentate	Documenti relativi a Commissario ad acta (nomina, compiti, rinnovo, cessazione e atti inerenti, ecc.)	ILLIMITATO	
	.02	Organismi direttivi e scientifici	Documenti relativi a Presidente e Consiglio di Amministrazione di Fondazione (nomina, compiti, rinnovo, cessazione e atti inerenti, convocazione, funzionamento, verbali sedute, ecc.)	ILLIMITATO	
	.02	Organismi direttivi e scientifici	Documenti relativi a Direttore Amministrativo, Sanitario, Sociale (nomina, compiti, rinnovo, cessazione e atti inerenti, ecc.)	ILLIMITATO	
	.02	Organismi direttivi e scientifici	Documenti relativi a Direttore Scientifico e componenti comitato (nomina, compiti, rinnovo, cessazione e atti inerenti, ecc.)	ILLIMITATO	
	.03	Organismi di controllo interno ed esterno	Documenti relativi a organi / organismi di controllo interno (nomina, sostituzioni, convocazioni, funzionamento, verbali sedute e atti inerenti, ecc.)	ILLIMITATO	
	.03	Organismi di controllo interno ed esterno	Documenti relativi a Organismo di vigilanza del Codice etico comportamentale (nomina, sostituzioni, convocazioni, ordini del giorno, verbali, ecc.)	ILLIMITATO	
	.03	Organismi di controllo interno ed esterno	Documenti relativi a organismi di controllo esterni (elezioni, sostituzioni, convocazioni, ordini del giorno, verbali, ecc.)	ILLIMITATO	
	.03	Organismi di controllo interno ed esterno	Documenti relativi al Collegio Sindacale (nomina, sostituzioni, convocazioni, funzionamento, verbali sedute e atti inerenti, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Collegio di Direzione (nomina, sostituzioni, convocazioni, funzionamento, verbali sedute e atti inerenti, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Consiglio dei sanitari (elezioni, sostituzioni, convocazioni, ordini del giorno, verbali, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Collegi tecnici (elezioni, sostituzioni, convocazioni, ordini del giorno, verbali, ecc.). Compresa quella relativa alla direzione dei distretti.	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Comitato Unico di Garanzia (elezioni, sostituzioni, convocazioni, ordini del giorno, verbali, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Comitato Etico (nomina, compiti, rinnovo dei componenti, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Conferenza dei Sindaci ed esecutivo (composizione ed elezione, cessazione e sostituzione, funzionamento, verbali sedute, interpellanze e mozioni, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Schede votazioni ed elezioni di collegi, comitati e commissioni	10 anni	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Commissione farmaceutica aziendale (nomina, compiti, rinnovo dei componenti, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Componenti Ufficio di Pubblica Tutela (nomina, compiti, rinnovo dei componenti, ecc.)	ILLIMITATO	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 1 - Area Amministrativa

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
3. Attività Giuridico-Legale	.01	Pareri, informative giuridiche e attività tecnico-legali	Pareri legali e relazioni tecniche, compresi quelli che la struttura predispone per altre strutture.	15 anni (se raccolta autonoma) se inserito in fascicolo per il tempo del procedimento	
	.02	Contenzioso legale	Contenzioso civile	ILLIMITATO	
	.02	Contenzioso legale	Contenzioso penale	ILLIMITATO	
	.02	Contenzioso legale	Contenzioso amministrativo	ILLIMITATO	
	.02	Contenzioso legale	Contenzioso giuslavoristico	ILLIMITATO	
	.02	Contenzioso legale	Contenzioso stragiudiziale (arbitrato, mediazione, ecc.)	ILLIMITATO	
	.02	Contenzioso legale	Contenzioso sanzioni amministrative attive (es.: sanzioni erogate dall'ente verso terzi in materia di igiene, veterinaria, sicurezza sul lavoro, osservanza normativa antifumo; sanzioni a strutture sanitarie, ecc.) e passive. Compresi gli scritti difensivi.	10 anni	
	.02	Contenzioso legale	Procedimento per riscossione ticket sanitari	10 anni (a partire dalla conclusione del procedimento)	
	.02	Contenzioso legale	Segnalazioni / Denunce / Querele all'Autorità Giudiziaria	ILLIMITATO	
	.03	Procedure concorsuali ed esecutive	Concordati, fallimenti, pignoramenti, recupero crediti, riscossione coatta, ecc.	10 anni	
	.03	Procedure concorsuali ed esecutive	Azioni di rivalsa	15 anni (dal ricovero / infortunio) in caso di avvenuto pagamento. 30 anni (dal ricovero / infortunio) negli altri casi.	In quanto l'azione di recupero del credito si prescrive in 5 anni, mentre il termine massimo di prescrizione del reato è di 30 anni. Se a seguito di azione di rivalsa è stato attivato un "contenzioso legale" si osserverà il termine previsto per tale categoria documentale.
	.04	Assicurazioni e gestione sinistri	Rapporto di brokeraggio assicurativo, RCT/O, gestione sinistri, polizze assicurative, richieste risarcimenti danni, tutela giudiziaria, furto incendi, infortuni, ecc.	ILLIMITATO	
	.04	Assicurazioni e gestione sinistri	Sinistri KasKo e RCA in assenza di contezioso	10 anni dall'avvenuta liquidazione	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 1 - Area Amministrativa

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Risorse Umane	.01	Dotazione organica e gestione del personale	Fabbisogni e Piante organiche del personale, Fluper, ecc. (si veda anche p. 7.05)	10 anni	
	.02	Concorsi e selezioni	Bandi, verbali di concorsi, selezioni, avvisi di mobilità, avvisi pubblici, graduatoria finale, ecc.	ILLIMITATO	
	.02	Concorsi e selezioni	Altri documenti inerenti la procedura concorsuale (<i>domande di partecipazione, documenti non ritirati dagli interessati, prove d'esame ed annesso materiale documentario</i>)	5 anni <i>dopo la scadenza della graduatoria</i>	
	.02	Concorsi e selezioni	Documentazione relativa alle procedure di valutazione comparativa per l'assunzione di personale sia a tempo determinato sia indeterminato.	10 anni (a partire dalla ratifica e salvo contenzioso in atto). I verbali conservazione ILLIMITATA.	
	.02	Concorsi e selezioni	Documentazione relativa all'elezione delle commissioni giudicatrici	10 anni (a partire dalla ratifica e salvo contenzioso in atto) ILLIMITATO i verbali	
	.03	Assunzioni, inquadramenti, incarichi e cessazione	Documenti relativi alla assunzione e prese in servizio dei dipendenti. Compresi i contratti, rinnovi, carteggio tra enti. Trattenimenti in servizio. Stato di servizio	ILLIMITATO	
	.03	Assunzioni, inquadramenti, incarichi e cessazione	Documentazione relativa al periodo di prova	ILLIMITATO (a conclusione, inserire nei fascicoli personali)	
	.03	Assunzioni, inquadramenti, incarichi e cessazione	Mobilità interna ed esterna (in entrata e in uscita)	ILLIMITATO	
	.03	Assunzioni, inquadramenti, incarichi e cessazione	Cessazione del rapporto per limiti di età, di servizio, volontarie	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.03	Assunzioni, inquadramenti, incarichi e cessazione	Documentazione relativa alle mansioni tipiche di ciascun ruolo, contratti di incarico, autorizzazioni per incarichi esterni, comunicazioni relative alla variazione dei dati personali, opzione per il regime di impegno a tempo pieno o a tempo parziale, opzione per attività intra-muraria o extra-muraria, assegnazione alla sede di servizio, ordini di servizio, cambio del settore disciplinare, riconoscimento mansioni superiori, modifica rapporto di lavoro, progressioni economiche orizzontali (PEO) e progressioni economiche verticali (PEV), Attribuzione / revoca / rinnovo qualifica di UPG, trasferimenti interni, libera professione (autorizzazione e atti conseguenti), ecc.	ILLIMITATO <i>(a conclusione, da inserire nei fascicoli personali)</i>	
	.04	Istituti contrattuali sospensivi della prestazione lavorativa	Documentazione relativa ai comandi e ai distacchi e alla ripresa di servizio nella sede originaria, aspettativa, congedi e altri istituti	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.05	Organizzazioni sindacali e contrattazione	Documenti legati ai rapporti con le rappresentanze sindacali e agli accordi di contrattazione nazionale e decentrata (verbali, <i>accordi</i>)	ILLIMITATO <i>(5 anni documentazione preparatoria: lettere di invito, comunicazioni e altra documentazione di supporto)</i>	
	.06	Retribuzioni e compensi	Atti e documenti in materia di inquadramento economico	ILLIMITATO	
	.06	Retribuzioni e compensi	Documentazione contabile relativa a: comandi, trasferimenti, mobilità, elementi accessori (lavoro straordinario, reperibilità, plus orario, incentivazioni, proventi, indennità rischio rx, missioni, trasferte, assegni famigliari, intramoenia, libera professione, altre competenze variabili), gestione buoni pasto, ecc.	10 anni	Armonizzato con stessa documentazione prodotta da altri enti locali.
	.06	Retribuzioni e compensi	Certificazioni dei redditi dipendenti e personale atipico	20 anni	
	.06	Retribuzioni e compensi	Documenti relativi a prestiti, cessioni di stipendio, delegazioni di pagamento, pignoramento presso terzi (a partire dall'estinzione del pagamento).	10 anni (dopo l'estinzione del debito)	
	.06	Retribuzioni e compensi	CUD	10 anni	
	.06	Retribuzioni e compensi	Tabulati mensili riepilogativi retribuzioni – variazioni <i>stipendiali</i> mensili (<i>cedolini paga</i>)	10 anni	
	.07	Trattamenti fiscali, contributivi e assicurativi	Trattamenti fiscali e contributivi del personale (Versamenti mensili CPDEL, INADEL, CPS, INPS/INPDAP, indennizzo INAIL per infortunio, ecc.)	ILLIMITATO	
	.07	Trattamenti fiscali, contributivi e assicurativi	Trattamento di fine rapporto/servizio (TFR, TFS)	ILLIMITATO (a conclusione, inserire nei fascicoli personali)	
	.07	Trattamenti fiscali, contributivi e assicurativi	Pratiche assicurative per infortunio	5 anni	
	.08	Inabilità al lavoro, invalidità, infermità, indennizzo	Dichiarazioni di infermità ed equo indennizzo, comprende le pratiche di riconoscimento di infermità per cause di servizio e l'equo indennizzo.	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 1 - Area Amministrativa

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Risorse Umane	.09	Presenze e assenze	Documenti relativi a permessi orari, assenze, ritardi, congedi ordinari e straordinari, ferie, congedo, cartellini / tabulati di presenza, permessi brevi e sindacali, sciopero, ecc.	5 anni	
	.09	Presenze e assenze	Riepilogo mensile rilevazione orari personale – timbrature	10 anni	
	.09	Presenze e assenze	Documenti relativi a turni ed orari di servizio, visite fiscali ai dipendenti	10 anni	
	.09	Presenze e assenze	Certificati malattia personale	10 anni (da cessazione attività)	
	.10	Quiescenza e relativo trattamento	Atti e documenti in materia di trattamento di quiescenza e di previdenza del personale, pratiche pensionistiche, riscatto e ricongiunzione servizi/ruolo, ecc.	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.11	Servizi a richiesta individuale	Pratiche di concessione benefici economici (ad es. per cure mediche) e di gestione delle provvidenze per il personale (contributi per asili nido, per centri estivi per figli di dipendenti, per abbonamenti ai mezzi di trasporto pubblico, ecc.), nonché le richieste di rilascio della tessera di riconoscimento e di certificati di servizio, l'assistenza fiscale su richiesta del dipendente.	10 anni	
	.12	Valutazione del personale	Procedimenti disciplinari, verbali ed atti del dirigente competente / ufficio procedimenti disciplinari	ILLIMITATO	
	.12	Valutazione del personale	Valutazione del personale (scheda valutazione)	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.12	Valutazione del personale	Documentazione riferita alle segnalazioni e alle comunicazioni sull'inosservanza dei doveri d'ufficio.	ILLIMITATO (a conclusione, inserire nel fascicolo personale)	
	.12	Valutazione del personale	Mobbing (denunce e segnalazioni)	ILLIMITATO (se nel fascicolo personale, 10 anni da cessazione attività altri esemplari)	
	.12	Valutazione del personale	Note di encomio, le congratulazioni per il servizio svolto e riconoscimenti simili	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.13	Formazione e aggiornamento del personale	Documentazione relativa ad attività formative (interna, esterna, a distanza) rivolte al personale (richieste, autorizzazioni, <i>documentazione presenze</i> , ecc.)	5 anni	
	.13	Formazione e aggiornamento del personale	Attestati di corsi di qualificazione e riqualificazione del personale	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.13	Formazione e aggiornamento del personale	Gestione crediti formativi professionali (ECM, ecc.)	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.13	Formazione e aggiornamento del personale	Piano annuale e triennale della formazione	10 anni	
	.14	Deontologia professionale ed etica del lavoro	Codici deontologici del personale, Codice Etico, codice di comportamento e iniziative connesse alla divulgazione, conoscenza e osservanza, iniziative di prevenzione in materia di anticorruzione.	ILLIMITATO	
	.15	Personale non strutturato o convenzionato	Pratiche di affidamento di incarichi di lavoro autonomo (incarichi libero professionali, incarichi di natura occasionale, co.co.co) e altre forme di lavoro atipico (incarichi, contratti e relazioni, ecc.).	ILLIMITATO (da inserire nel fascicolo <i>personale</i>)	
	.15	Personale non strutturato o convenzionato	Documenti relativi alla presa in servizio e alla cessazione di personale atipico (collaboratori, stagisti, specializzandi, frequentatori, dottorandi, tirocinanti, volontari, <i>borsisti</i> , ecc.). Compresi i contratti, affidamento di incarichi, rinnovi, carteggio tra enti.	ILLIMITATO (da inserire nel fascicolo <i>personale</i>)	
	.15	Personale non strutturato o convenzionato	Fascicolo rapporti convenzione (MMG, PdF, Sumai, ecc.)	ILLIMITATO	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 1 - Area Amministrativa

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
5. Risorse finanziarie e gestione contabile	.01	Attività finanziaria e contabile	Budget di cassa (rendiconto finanziario)	10 anni	
	.01	Attività finanziaria e contabile	Ordinativi / Distinte di incasso e di pagamento, documentazione relativa alla gestione della spese (impegno, liquidazione, ordinazione e pagamento) e altre registrazioni contabili di carattere transitorio (mandati / reversali, movimenti del tesoriere, ecc.)	10 anni dall'approvazione del bilancio (se esistono per gli anni corrispondenti i registri contabili)	Sarà possibile scartare dopo 2 anni eventuale documentazione prodotta in copia
	.01	Attività finanziaria e contabile	Verballi e verifiche Cassa	ILLIMITATO	
	.01	Attività finanziaria e contabile	Convenzioni, attivazione e cessazione con istituti di credito	10 anni	
	.01	Attività finanziaria e contabile	Servizi bancari telematici (internet banking)	10 anni	
	.01	Attività finanziaria e contabile	Estratti conto operazioni bancarie	10 anni	
	.01	Attività finanziaria e contabile	Registri contabili principali, anche sotto forma di banche dati (mastro, giornali di cassa, ecc.)	ILLIMITATO	
	.02	Bilancio e Rendicontazione	Bilanci e rendiconto della gestione con i relativi allegati	ILLIMITATO	
	.02	Bilancio e Rendicontazione	Bilancio: carteggio interlocutorio interno, assegnazione budget, ecc.	10 anni	
	.02	Bilancio e Rendicontazione	Situazioni contabili periodiche (CET)	15 anni (se raccolta autonoma, se invece inserito in fascicolo per il tempo del procedimento)	
	.02	Bilancio e Rendicontazione	Libro cespiti	ILLIMITATO	
	.03	Gestione entrate-uscite	Documentazione varie inerenti il flusso degli incassi (avvisi di riscossione)	10 anni	
	.03	Gestione entrate-uscite	Cartelle pagamenti esattoriali	10 anni (se esistono per gli anni corrispondenti i registri contabili / libro giornale)	
	.03	Gestione entrate-uscite	Fatture emesse e fatture ricevute	10 anni (se esistono per gli anni corrispondenti i registri contabili / libro giornale)	
	.03	Gestione entrate-uscite	Solleciti di pagamento	10 anni	
	.03	Gestione entrate-uscite	Documentazione relativa ricognizione debiti/crediti gestione liquidatoria	ILLIMITATO	
	.03	Gestione entrate-uscite	Cessioni del credito	10 anni	
	.03	Gestione entrate-uscite	Rimborsi spese non dovute	10 anni	
	.04	Gestione fiscale e imposte	Documenti relativi a imposte e tasse dell'azienda quale sostituto di imposta IRES, ICI, IMU, IRPEF, bollo virtuale, IVA ecc.	10 anni	
	.04	Gestione fiscale e imposte	Registro IVA vendite, acquisti	ILLIMITATO	
	.04	Gestione fiscale e imposte	Certificazioni ritenute d'acconto	10 anni	
	.04	Gestione fiscale e imposte	Modello 770 (dichiarazione sostituti d'imposta)	10 anni	
	.04	Gestione fiscale e imposte	Modello Unico (redditi IRAP e IVA)	10 anni	

MASSIMARIO DEL SISTEMA SOCIOSANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIOSANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 1 - Area Amministrativa

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
6. Gestione e organizzazione del patrimonio	.01	Progettazione e costruzione di beni immobili con relativi impianti	Documentazione relativa alla progettazione e realizzazione degli immobili dell'azienda e alla relativa impiantistica (progettazione, direzione lavori, collaudi, contratti, planimetrie, progetti di costruzione, ecc.). Comprese le procedure di gare d'appalto per la realizzazione di dette opere / impianti.	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.02	Acquisizione e gestione beni immobili e relativi servizi	Documentazione relativa ai procedimenti per l'acquisto di terreni, edifici, strutture e immobili di vario tipo, nonché la loro destinazione d'uso e l'ordinaria gestione patrimoniale. Compresi gli atti e documenti comprovanti la proprietà di immobili, la gestione di lasciti, nonché l'inventario beni immobili.	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.02	Acquisizione e gestione beni immobili e relativi servizi	Documentazione relativa agli adempimenti necessari per la gestione delle locazioni attive e passive di immobili, comodati, ecc.	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.02	Acquisizione e gestione beni immobili e relativi servizi	Documentazione che si riferisce alla alienazione, vendita, cessione o permuta di immobili, compresa l'eventuale indizione e gestione di asta pubblica	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.02	Acquisizione e gestione beni immobili e relativi servizi	Documentazione relativa a costituzione e/o trasferimento di diritti reali sugli immobili (superfici, servitù)	ILLIMITATO	
	.02	Acquisizione e gestione beni immobili e relativi servizi	Programma triennale ed elenco annuale lavori pubblici	ILLIMITATO	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Documentazione relativa all'acquisizione e fornitura di beni mobili, di materiali e attrezzature tecniche, scientifiche, e non, e per la fornitura di servizi, compresi contratti RCA auto (richieste partecipazione e gare, bandi gara, offerte, verbali seduta, atti indizione e aggiudicazione, contratti, ecc.)	10 anni <i>dalla data di dismissione del bene</i>	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Acquisizione e gestione di beni mobili da lasciti o donazioni	ILLIMITATO	<i>La documentazione relativa a donazioni di beni mobili anche a carattere artistico deve essere classificata all'interno della voce donazione e conservata a tempo illimitato. Eventuali raccolte documentali spurie relative all'acquisizione/gestione di beni mobili di carattere artistico è da conservare a tempo illimitato.</i>
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Servizi di vigilanza, portineria, automezzi, ecc.	ILLIMITATO	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Inventario beni mobili: Libro cespiti ammortizzabili e trasferimenti interni beni inventariati.	ILLIMITATO (per Libro cespiti, altra documentazione 10 anni)	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Albo fornitori	20 anni	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Documentazione relativa agli adempimenti necessari per la gestione delle locazioni attive e passive di beni mobili e comodati	ILLIMITATO	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Documentazione che si riferisce alla alienazione, cessione o permuta di beni mobili, compresa eventuale indizione e gestione di asta pubblica. Fuori uso.	10 anni	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Utenze varie (telefono, acqua, gas, calore, illuminazione, ecc.;	10 anni	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Servizio ristorazione, mensa e ticket pasti (rapporti con fornitore)	10 anni	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Documentazione relativa all'attività dei magazzini (richieste a magazzino, documento di trasporto, ordini, inventario di magazzino, registri carico-scarico, ecc.)	5 anni (per richieste a magazzino; tutto il resto 10 anni)	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 1 - Area Amministrativa

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
6. Gestione e organizzazione del patrimonio	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documentazione relativa alle procedure di appalto per la ristrutturazione, manutenzione, restauro di immobili. Compresi progettazione e collaudi relativi a lavori effettuati su edifici.	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documenti relativi alle eventuali modifiche della destinazione d'uso, ecc.;	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documentazione relativa alle procedure di appalto per la ristrutturazione, manutenzione, restauro di impianti. Compresa certificazione di manutenzione di impianti.	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documenti che si riferiscono alla manutenzione e riparazione di tutti i beni mobili (arredi, fax PC, scanner, ecc.), compresi i collaudi relativi ad apparecchiature, contratti di manutenzione, esiti delle manutenzioni.	20 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documenti che si riferiscono alla manutenzione e riparazione di apparecchiature elettromedicali, di laboratorio e biomediche	20 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Interventi abbattimento barriere architettoniche	20 anni	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documentazione inerente posizionamento e rimozione cartelli indicatori e segnaletica	10 anni	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documenti su piccoli interventi tecnici (falegnameria, idraulica, ecc.)	5 anni	
	.05	Attività contrattuale e tutela della proprietà intellettuale	Contratti attivi (Concessioni, sponsorizzazioni, ecc.)	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.05	Attività contrattuale e tutela della proprietà intellettuale	Ricerca (contratti di ricerca, <i>contratti</i> di sperimentazione clinica, ecc.)	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.05	Attività contrattuale e tutela della proprietà intellettuale	Brevetti (documentazione inerente il rilascio, la gestione, la titolarità, il deposito, la durata, gli atti di disposizione, ecc.)	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.06	Sicurezza degli ambienti di lavoro	Documentazione relativa alla sicurezza dei luoghi di lavoro e degli impianti a essi afferenti (adempimenti, sicurezza apparecchiature elettriche, procedure 1° soccorso, gestione e valutazione del rischio, impianti antintrusione, nomina addetti prevenzione e protezione RSPP, formazione su sicurezza e squadre di emergenza).	20 anni (dalla cessazione dell'attività o modifica alla titolarità di esercizio e modifica dei locali)	
	.06	Sicurezza degli ambienti di lavoro	Documenti previsti dalla normativa in materia di sicurezza sul lavoro e prevenzione (ad es. i vari piani per la sicurezza dei luoghi di lavoro, la nomina dei responsabili per la sicurezza, ecc.), compresa la formazione specifica del personale dipendente.	20 anni (dalla cessazione dell'attività o modifica alla titolarità di esercizio e modifica dei locali)	
	.06	Sicurezza degli ambienti di lavoro	Sorveglianza sanitaria e sicurezza ambiente di lavoro: rapporti e verbali di sopralluogo	ILLIMITATO	
	.06	Sicurezza degli ambienti di lavoro	Visite mediche del personale e attestazioni di idoneità	ILLIMITATO	
	.07	Gestione dei rifiuti	Documenti che si riferiscono alla gestione e smaltimento dei rifiuti dell'ente, anche quelli speciali, tossici, nocivi e biologici. Rientra in questa classe anche la nomina degli addetti responsabili.	20 anni	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 1 - Area Amministrativa

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
7. Sistemi Informativi e comunicazione	.01	Sistema documentale	Documentazione relativa alla gestione del servizio archivistico e strumenti di corredo. Compresi: manuale di gestione documenti, gestione del protocollo, gestione degli archivi (procedure di scarto, titolari , massimari, richieste di consultazione), ecc.	ILLIMITATO	Si conservano a tempo illimitato anche: registro di protocollo, repertorio dei fascicoli, registro albo on-line, registri: protocollo, fascicoli, albo on line, notifiche, ordinanze, decreti, deliberazioni, determinazioni, contratti e tutte le tipologie di registri e repertori previsti dalla legge o regolamenti. Nel caso di incertezza sulla loro conservazione si deve sempre esprimere la Soprintendenza archivistica.
	.01	Sistema documentale	Albo on line e pubblicazioni su siti web aziendali relativamente alle leggi in materia di accesso e trasparenza nella pubblica amministrazione	2 anni per Albo on line; per altre tipologie di documentazione si deve fare riferimento alle leggi in materia e alle disposizione dei Garanti/Autorità	
	.01	Sistema documentale	Domande consultazione archivio	1 anno	
	.01	Sistema documentale	Richieste di accesso ai documenti e conseguenti provvedimenti	1 anno per fini amministrativi ILLIMITATO (per motivi di studio o informazione archivistica)	Se la domanda di accesso produce diniego, e conseguente ricorso, la documentazione deve essere trasferita nell'eventuale fascicolo di contenzioso e conservata per il tempo dello stesso. Per la gestione delle domande di accesso agli atti si possono prevedere due modelli: centralizzato e decentralizzato. Centralizzato: tutta la documentazione è gestita in un unico fascicolo da un ufficio preposto. Decentralizzato: ogni domanda è gestita all'interno del fascicolo del procedimento dal relativo responsabile, si conserva per il tempo del fascicolo stesso.
	.02	Rapporti con il pubblico, sportelli informativi e trasparenza	Relazioni con il pubblico: gestione segnalazioni, reclami e apprezzamenti, informazioni, pubbliche relazioni	10 anni	
	.02	Rapporti con il pubblico, sportelli informativi e trasparenza	Comunicazione con i media, rassegna stampa, conferenze stampa,	1 anno	
	.02	Rapporti con il pubblico, sportelli informativi e trasparenza	Pubblicazioni aziendali, Piano di Comunicazione, guida ai servizi	ILLIMITATO	
	.02	Rapporti con il pubblico, sportelli informativi e trasparenza	Documenti relativi alla rappresentanza istituzionale (eventi, patrocinî, manifestazioni, ecc.)	5 anni	
	.03	Tutela della riservatezza	Aggiornamenti elenchi incaricati privacy, nomina incaricati	10 anni	
	.03	Tutela della riservatezza	Informativa dell'Azienda e consenso al trattamento dati	Medesimo tempo di conservazione della documentazione relativa al prestazione/procedimento reso	Se il consenso (e l'informativa) è collegato a più documentazione deve essere conservato fino all'avvenuto scarto di tutti i documenti a cui afferisce.
	.03	Tutela della riservatezza	Documentazione relativa ai Reclami per la tutela della Privacy. Compresa sia la domanda (reclamo presentato) sia la risposta fornita	10 anni	
	.04	Biblioteche e centri di documentazione	Documentazione relativa al servizio di biblioteca, acquisti, catalogazione, richieste di consultazione e prestito, ecc. Compresa la gestione del centro di documentazione.	5 anni	
	.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla gestione delle banche dati (es. sistema di gestione del personale, sistema finanziario-contabile, ecc.)	ILLIMITATO	Si intende la documentazione relativa alle fasi di progettazione e di gestione delle banche dati come sistema in quanto tale; da non confondere con i dati immessi che possono essere assoggettati a tempi diversi di conservazione.
	.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla realizzazione e gestione delle reti interne ed esterne (comprese le cablature, gli impianti di rete, etc.), nonché la loro manutenzione e gli interventi per il loro corretto funzionamento.	10 anni	
	.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla sicurezza informatica	ILLIMITATO	
	.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla gestione dell'attività di informatizzazione e richieste di abilitazione e intervento	5 anni	
	.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla realizzazione e gestione del SISS (es. progettazione e architettura sistemi, integrazione, installazione e configurazione sistemi, gestione carte, ecc.)	10 anni	
	.05	Sistema informatico, reti e sicurezza	Documentazione inerente i sistemi dedicati alle attività CUP/ Call Center Regionale anche per la libera professione	10 anni	
	.06	Statistiche e reporting	Statistiche e report istituzionali (es. flussi informativi ministeriali, regionali, ISTAT, ecc.) a fronte di richieste di enti esterni	ILLIMITATO	

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
1. Organizzazione territoriale	.01	Gestione e organizzazione dipartimentale e interdipartimentale, distrettuale ed interdistrettuale	Atti di indirizzo, coordinamento e programmazione attività dipartimentali e distrettuali Progetti (atti di approvazione) Rapporti con organi interni ed esterni	ILLIMITATO	
	.01	Gestione e organizzazione dipartimentale e interdipartimentale, distrettuale ed interdistrettuale	Monitoraggio attività dipartimentali e distrettuali	5 anni	Si tratta di documentazione di carattere ordinario/rutinario (fogli di lavoro e verbali di carattere operativo). I documenti relativi alla gestione delle attività, al funzionamento ed all'organizzazione dei dipartimenti e dei distretti rientrano in Atti di indirizzo, coordinamento e programmazione attività dipartimentali e distrettuali (Il.1.01)
	.01	Gestione e organizzazione dipartimentale e interdipartimentale, distrettuale ed interdistrettuale	Verbalì incontri / riunioni interne di pianificazione e organizzazione	10 anni	
	.02	Progetti, interventi e iniziative varie dipartimentali / distrettuali	Documentazione istruttoria relativa a progetti	10 anni	Il progetto è conservato illimitatamente (Il.1.01) (decreto di approvazione progetto, approvazione graduatoria ed erogazione contributi); mentre la documentazione istruttoria concerne: istanze/domande; valutazioni si può scartare a 10 aa. Come "gare appalto" (Vedi I.6.03).
	.03	Coordinamento e gestione personale infermieristico, tecnico-assistenziale, di prevenzione	Documenti inerenti attività del personale (turni di attività, assegnazioni, segnalazioni, compiti assegnati, obiettivi, ecc.). La documentazione relativa al rapporto di lavoro, alla valutazione del personale, ecc. dovrà essere classificata e conservata secondo quanto specificato nelle voci di classificazione del titolo 1.	5 anni	

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
2. Prevenzione e sicurezza negli ambienti di lavoro	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione, ecc.)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/rutinaria interna ed esterna attività prevenzione e sicurezza negli ambienti di lavoro	5 anni	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione inerente attività formativa da parte dei soggetti accreditati da Regione Lombardia	10 anni	
	.02	Medicina del lavoro e malattie professionali	Certificati idoneità lavorativa specifica alle mansioni rilasciati dallo PSAL	10 anni	
	.02	Medicina del lavoro e malattie professionali	Ricorso avverso giudizi idoneità / inidoneità specifica alla mansione rilasciati dal Medico Competente con relativa documentazione sanitaria sul lavoratore	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Certificato di idoneità lavorativa di minori (D.Lgs. 345/99)	10 anni	
	.02	Medicina del lavoro e malattie professionali	Accertamenti sanitari e strumentali di idoneità/inidoneità al lavoro effettuati da medici competenti delle ditte	10 anni	
	.02	Medicina del lavoro e malattie professionali	Inchieste sulle malattie professionali (richieste, relazione, sopralluogo, rapporto a procura, ecc.)	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Cartella sanitaria e di rischio del lavoratore (accertamenti sanitari, referti, giudizio di idoneità al lavoro o cambio mansioni lavorative, accertamenti specialistici ulteriori, ecc.)	10 anni dalla cessazione del rapporto di lavoro. Salvo nei casi di: - esposizione ad agenti biologici: 10 anni dalla cessazione, ma fino a 40 anni dalla cessazione per infezioni latenti, recrudescenti, ecc.; - esposizione a radiazioni ionizzanti: 30 anni dalla cessazione; - esposizione ad agenti cancerogeni: 40 anni dalla cessazione.	D.lgs. 81/2008 art. 243 - art. 280 - Decreto Ministero della Salute 12 Luglio 2007, n.155: art. 3
	.02	Medicina del lavoro e malattie professionali	Certificato medico di malattia professionale (Mod. 5 SS INAIL)	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Denunce / Segnalazione malattia professionale da parte del medico (Mod. 92 bis INAIL)	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Segnalazione dell'ISPEL (Sistema sorveglianza epidemiologica Mal. Prof. SW nazionale)	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Scheda OCCAM (OCcupational CAncer Monitoring) ISPEL - INT	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Questionario sulla storia di lavoro e sulle abitudini di vita - Centro Operativo Lombardia (mesotelioma)	ILLIMITATO se in fascicolo personale. 30 anni da cessazione attività	
	.02	Medicina del lavoro e malattie professionali	Questionario sulla storia di lavoro e sulle abitudini di vita - ReNaTuNS Registro Reg. Lombardia	ILLIMITATO se in fascicolo personale. 30 anni da cessazione attività	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
2. Prevenzione e sicurezza negli ambienti di lavoro	.03	Igiene e sicurezza sul lavoro	Attività di vigilanza sanitaria sull'applicazione delle norme in materia di sicurezza ed igiene del lavoro negli ambienti di lavoro (segnalazioni, denunce, verbali di sopralluogo, verbale sanzionatorio, ecc.)	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Certificazioni / pareri igienico-sanitari su progetti nuovi insediamenti produttivi di carattere industriale e artigianale (es. SCIA ambienti di lavoro)	30 anni	Insedimenti produttivi di tipo industriale / artigianale: 30 anni dalla certificazione / SCIA
	.03	Igiene e sicurezza sul lavoro	Certificazioni / pareri igienico-sanitari su progetti di altri insediamenti produttivi di carattere non industriale (es. SCIA ambienti di lavoro)	5 anni	Altri insediamenti di tipo commerciale: 5 anni dalla certificazione/SCIA (es. parrucchiere, estetista, tatuatori, ecc.)
	.03	Igiene e sicurezza sul lavoro	Trattamento rifiuti speciali non pericolosi / pareri (art. 208 d.lgs. 152/2006) e altra documentazione	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Campionamenti ambientali per la determinazione quali-quantitativa fattori di rischio (rumore, microclima, polveri, agenti chimici, vibrazioni)	ILLIMITATO verbali; 10 anni altra documentazione	
	.03	Igiene e sicurezza sul lavoro	Autorizzazione: lavoro in locali interrati /seminterrati. in deroga art. 65 D.lgs. 81/08	2 anni dalla data di cessazione di attività	
	.03	Igiene e sicurezza sul lavoro	Inchiesta infortuni (comprendente: denunce, relazione di sopralluogo, esecuzione di rilievi, verbale raccolta di sommarie informazioni testimoniali, verbale raccolta di dichiarazioni spontanee, certificato medico di infortunio lavorativo, invito a presentarsi, richiesta di documentazione, acquisizione di documentazione, scheda "Inchiesta infortuni", verbale di accertamento e contestazione illecito amministrativo, ecc.)	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Referti infortuni che non esitano in indagine	10 anni	
	.03	Igiene e sicurezza sul lavoro	Registro infortuni	4 anni dall'ultima registrazione e, se non usato, dalla data in cui è stato vidimato	D.M. 12/9/58, art.2
	.03	Igiene e sicurezza sul lavoro	Rapporto relativo all'infortunio sul lavoro alla Procura della Repubblica con allegato l'inchiesta	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Fascicolo prevenzione infortuni	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Bonifica amianto (segnalazioni dei casi esposti, certificato esposizione, certificato PSAL per accesso benefici INAIL- INPS,	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Bonifica amianto (notifica amianto in strutture o luoghi, piano di lavoro per la bonifica, verbale di controllo c/o siti con presenza amianto e/o ditte abilitate a smantellamento, verbale sanzionatorio, relazione annuale bonifica / smantellamento amianto delle ditte, ecc.).	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Registro esposti ed ex esposti amianto	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Registro degli esposti ad agenti cancerogeni e registro degli esposti ad agenti biologici	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Registro informatico "Progetto rilevazione amianto" / notifiche censimento amianto	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Patentino per bonificatore amianto	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Comunicazioni per detrazioni fiscali	10 anni	
	.03	Igiene e sicurezza sul lavoro	Comunicazioni aziende classe di rischio primo soccorso (dm 388/2008)	10 anni	
	.03	Igiene e sicurezza sul lavoro	Comunicazioni nomina RLS e RSPP	5 anni	
	.03	Igiene e sicurezza sul lavoro	Rilascio patentini di abilitazione utilizzo gas tossici (compresi verbali esami) e relative revisioni	5 anni	RD n. 147/1927
	.03	Igiene e sicurezza sul lavoro	Comunicazioni relative alla notifica preliminare cantieri	5 anni	
	.03	Igiene e sicurezza sul lavoro	Verbali di ispezione e controlli cantieri	5 anni; 10 anni nel caso di contenzioso (sanzioni) dalla proposta di archiviazione	
	.04	Sicurezza e impiantistica	Documentazione relativa alle attività di vigilanza sulla sicurezza dei luoghi di lavoro delle macchine / impianti / attrezzature di lavoro	ILLIMITATO verbali; 10 anni dalla demolizioni degli impianti e/o delle attrezzature altra documentazione	
	.04	Sicurezza e impiantistica	Documentazione inerente presunte non conformità macchine / attrezzature marcatura CE	ILLIMITATO	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
3. Prevenzione medico - sanitaria	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione, ecc.)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria / routinaria interna ed esterna attività di prevenzione medico-sanitaria	5 anni	
	.02	Educazione sanitaria	Progetti di promozione della salute	ILLIMITATO	
	.02	Educazione sanitaria	Documentazione istruttoria e corrispondenza relativa a progetti ed interventi di educazione alla salute.	10 anni	
	.02	Educazione sanitaria	Materiale informativo (compresi i questionari) per promozione ed educazione alla salute	1 anno	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Documenti su attività di disinfezione/disinfestazione (denunce / segnalazioni, convenzione con enti, verbale di controllo, scheda intervento, ecc.)	ILLIMITATO convenzioni, denunce e verbali; 10 anni altra documentazione	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Notifiche e denunce malattie infettive (scheda notifica)	10 anni	DM 15/12/90 (Sistema informativo delle malattie infettive e diffusive) DM 29/7/98 (Modifiche relative alla TBC)
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Registro informativo malattie infettive (MAINF)	ILLIMITATO	DM 15/12/90 (Sistema informativo delle malattie infettive e diffusive) DM 29/7/98 (Modifiche relative alla TBC)
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Indagine / Inchiesta / Sorveglianza epidemiologica di malattia infettiva (esiti campionamento, relazione sanitaria, dati su epidemia, elenco contatti, profilassi prescritta, comunicazione a enti locali e/o H, ecc.)	10 anni da ultima registrazione	Circ. Min. Sanità n. 61 del 19/12/1986. In considerazione del termine di prescrizione del diritto al risarcimento del danno subito da un paziente che è di dieci anni, siffatta documentazione verrà conservata sino al compimento della prescrizione decennale
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Indagine / Inchiesta / Sorveglianza epidemiologica di malattia infettiva (referto visite, esami laboratorio e strumentali, ecc.)	10 anni da ultima registrazione	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Attuazione campagne vaccinali (calendarizzazione, inviti e registrazione vaccinazioni, ecc.)	ILLIMITATO i Registri e le schede vaccinali; 2 anni altra documentazione (compresi i fogli di lavoro)	Nota RL prot. H1.2001.0033136 del 16.05.2001 Direzione generale degli archivi. Prontuari di scarto per le ASL
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda anamnesi prevaccinale	ILLIMITATO	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Consenso informato alla vaccinazione	ILLIMITATO	Circ. Min. Sanità n. 61 del 19/12/1986
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Registro vaccinazioni	ILLIMITATO	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda vaccinale individuale cartacea o informatizzata con i dati vaccinazioni eseguite (data, nome commerciale, lotto, controllo di stato, data di scadenza del prodotto, ecc.)	Collegato all'esistenza in vita del soggetto cui si riferisce la scheda (fino a 5 anni dopo il decesso del vaccinato)	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Convocazione vaccinazioni obbligatorie (previste dal Piano aziendale vaccinale)	ILLIMITATO il Registro; 2 anni altra documentazione	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda informativa sui danneggiati da vaccinazioni	ILLIMITATO	Circolare del Ministero della Sanità 10 aprile 1992
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Segnalazione reazioni avverse a vaccini	ILLIMITATO	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Richiesta forniture vaccini (ordinativo)	2 anni	Nota RL prot. H1.2001.0033136 del 16.05.2001 Direzione generale degli archivi. Prontuari di scarto per le ASL
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Registrazione temperature frigoriferi per vaccini	1 anno	Nota RL prot. H1.2001.0033136 del 16.05.2001
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Registrazione interruzione catena freddo per vaccini	10 anni	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Vaccinazione in ambiente protetto (richieste, comunicazioni)	10 anni	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda AIDASS di valutazione funzionale globale pazienti AIDS	ILLIMITATO	DGR 7/6471 del 2001
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Piano di assistenza personalizzato per HIV/AIDS extra-H	5 anni dall'ultima prestazione	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Registro Regionale SOFIA (dati scheda extra-H)	ILLIMITATO	DGR 7/6471 del 2001
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Anamnesi specifica per malattie a trasmissione sessuale	10 anni	Nota RL prot. H1.2001.0033136 del 16.05.2001 Direzione generale degli archivi. Prontuari di scarto per le ASL
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Fascicolo ambulatoriale per malattie a trasmissione sessuale (MTS / HIV) (Scheda accoglienza / informativa, diario clinico, referti, visite, esami laboratorio e strumentali, consenso informato al trattamento, ecc.)	10 anni dalla chiusura del fascicolo	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda sorveglianza infezione da HIV	10 anni da ultima registrazione	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda notifica MTS	10 anni	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda consulenza linea informativa telefonica MTS / HIV (help line telefonica)	5 anni	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Bollettini epidemiologici malattie infettive (report di epidemia)	5 anni dalla cessazione dell'allerta	
	.04	Prevenzione malattie cronico-degenerative	Gestione screening (campagne, esito screening, referti, ecc.)	10 anni	
	.04	Prevenzione malattie cronico-degenerative	Gestione screening (inviti e solleciti)	3 anni	
	.04	Prevenzione malattie cronico-degenerative	Indagine / Inchiesta / Sorveglianza epidemiologica	10 anni dalla chiusura del fascicolo	
	.04	Prevenzione malattie cronico-degenerative	Registri anatomia patologica (copie)	5 anni	
	.04	Prevenzione malattie cronico-degenerative	Registro mortalità e schede morte ISTAT	ILLIMITATO	
	.04	Prevenzione malattie cronico-degenerative	Registro tumori	ILLIMITATO	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
3. Prevenzione medico - sanitaria	.05	Igiene urbana, ambientale e sanità pubblica	Documenti relativi a pareri su progetti di edilizia privata e pubblica (compreso rilascio pareri)	10 anni	Procedimento relativo al parere e non alla gestione dell'intera pratica edilizia in capo ad altri enti (comune, provincia, ARPA, ecc.)
	.05	Igiene urbana, ambientale e sanità pubblica	Tombe di privati (richiesta, pareri igienico-sanitari)	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Urbanistica (valutazione igienico sanitaria, richiesta e pareri da enti)	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Pareri, Autorizzazioni e relativi controlli su realizzazione ed esercizio strutture sanitarie, socio-sanitarie pubbliche e private (es. Centri Procreazione Medicalmente Assistita - PMA, Strutture di ricovero e cura, Residenzialità psichiatrica)	ILLIMITATO (fino a cessazione di attività o modifiche di titolarità di esercizio – subingressi)	
	.05	Igiene urbana, ambientale e sanità pubblica	Pareri per esercizio di attività commerciali, artigiane, alberghi e strutture extra alberghiere, sportive (piscine) e ludico-ricreative	ILLIMITATO (fino a cessazione di attività o modifiche di titolarità di esercizio – subingressi)	
	.05	Igiene urbana, ambientale e sanità pubblica	Certificati di idoneità dei carri funebri	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Pareri di insalubrità / inabitabilità edifici ad uso pubblico e/o privato	10 anni se civili abitazioni, ILLIMITATO se insediamenti produttivi	
	.05	Igiene urbana, ambientale e sanità pubblica	Certificati di idoneità igienico-sanitaria di edifici ad uso pubblico e privato	10 anni se civili abitazioni, ILLIMITATO se insediamenti produttivi	
	.05	Igiene urbana, ambientale e sanità pubblica	Accertamento delle condizioni igienico-sanitarie e di sicurezza edifici/strutture ad uso pubblico e privato, comprese le strutture scolastiche e penitenziarie (verbali di ispezione/sopralluogo) ed eventuali prescrizioni	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Documentazione sulle radiazioni ionizzanti - RI (per usi industriale, di ricerca, sanitario). Comunicazione preventiva ex art. 22 e 24 D.lgs. 230/95, nulla osta di cat. B ex art 29, procedimenti ex art 30, revoca autorizzazione ex art. 146, vigilanza radiazioni ionizzanti, ecc. Compresa la documentazione relativa ai dosimetri personali.	ILLIMITATO se in fascicolo personale / ditta o impresa; altrimenti 30 anni da cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Documenti in tema ambientale, tossicologia, radioprotezione (denunce, esposti, accertamenti, verbali sopralluogo e sanzionatorio)	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Documentazione inerente ritrovamento, messa in sicurezza e smaltimento materiale radioattivo	10 anni dalla data di chiusura del procedimento	
	.05	Igiene urbana, ambientale e sanità pubblica	Analisi rischio siti contaminati	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Valutazione Impatto Ambientale (VIA) e Valutazione Ambientale Strategica (VAS)	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Parere per interventi di bonifica e ripristino ambientale	10 anni dall'avvenuta bonifica	D.Lgs. 152/2006 e s.m.i
	.05	Igiene urbana, ambientale e sanità pubblica	Documenti sulle radiazioni non ionizzanti (NIR) (elettrosmog). Denunce, esposti, segnalazioni, vigilanza di emissioni elettromagnetiche non ionizzanti (NIR)	ILLIMITATO se in fascicolo personale / ditta o impresa; altrimenti 30 anni da cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Autorizzazione e installazione Risonanza Magnetiche (RM)	2 anni dalla data di comunicazione cessazione di utilizzo	
	.05	Igiene urbana, ambientale e sanità pubblica	Movimentazione sorgenti radiogene, trasporto e commercio sostanze radioattive	ILLIMITATO se in fascicolo personale / ditta o impresa; altrimenti 30 anni da cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Registro carico - scarico rifiuti speciali, integrati con i formulari relativi al trasporto dei rifiuti	5 anni dalla data dell'ultima registrazione	D.Lgs. 22/97 art.12 e s.m.i. (art. 190 del D.Lgs 152/2006 come modificato dalla legge 125/2013)
	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni / controlli acque di balneazione	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni / controlli gas tossici (e relativi pareri)	ILLIMITATO	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
3. Prevenzione medico - sanitaria	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni / controlli fitofarmaci	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Produzione e/o commercializzazione di prodotti cosmetici (notifica immissione in commercio o importazione, comunicazione cessazione ditte, elenco cosmetici commercializzati e importati)	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingresso)	
	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni/controlli su prodotti cosmetici (verbale di controllo, prescrizioni, comunicazione a NAS e Polizia Giudiziaria, ecc.)	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Valutazioni di effetti sulla salute di esposizione a fattori di rischio ambientale	ILLIMITATO se in fascicolo personale / ditta o impresa; altrimenti 30 anni da cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni/controlli su piscine (parere igienico-sanitario per apertura piscine, verbale sopralluogo, prelevamento campioni, analisi ed eventuali prescrizioni, ecc.)	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Verbale di controllo / sopralluogo per idoneità alloggiativa ed eventuali prescrizioni	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Segnalazione all'autorità giudiziaria dei rischi connessi per gli impianti termici nei casi di intossicazione da CO	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Segnalazione intossicazione CO diagnosticati da parte dei Dipartimenti emergenza H	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Parere igienico-sanitario per rilascio autorizzazioni (istanze, relazioni tecniche, planimetrie, atti istruttori copie atti autorizzativi, ecc.)	30 anni dalla cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Proposta ordinanza al Sindaco per inconvenienti igienico - sanitari (proposta, ordinanza, verifica ottemperanza, ecc.)	10 anni <i>dalla conclusione del procedimento</i>	
	.05	Igiene urbana, ambientale e sanità pubblica	Autorizzazione al seppellimento di feti e parti anatomiche e relativa richiesta	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Registro dei parti e Registro degli aborti	ILLIMITATO	L'adozione di questi due registri risale al R.D. 6 dicembre 1928 n. 3318 (Istituzione del Regolamento per l'esercizio ostetrico delle levatrici). La compilazione dei registri viene confermata dal R.D. 26 maggio 1940 n. 1364 (che abroga il R.D. n.3318/28) e successivamente richiamata dal D.P.R. n. 163 del 7/3/1975 (che abroga il R.D. n. 1364/40). Con la Legge n. 42 del 26/02/1999 viene abrogato il DPR n.163/75 e di conseguenza i due registri. I registri sono a conservazione illimitata e il loro contenuto deve rimanere segreto.
	.05	Igiene urbana, ambientale e sanità pubblica	Copie di Elenchi deceduti (<i>dai registri degli</i> enti locali)	2 anni	<i>Elenchi dei defunti per i quali è stato fissato il funerale il giorno dopo</i>
	.05	Igiene urbana, ambientale e sanità pubblica	Passaporti mortuari da parte di enti locali e relativa richiesta	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Passaporti mortuari rilasciati e relativa richiesta	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Pareri e relativa richiesta per scuole di formazione, strutture turistico ricreative, servizi alla persona	30 anni dalla cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni e controlli su scuole di formazione, strutture turistico ricreative, servizi alla persona (verbale di controllo / sopralluogo ed eventuali prescrizioni, denunce, esposti, ecc.)	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Verifica periodica condizioni igienico sanitarie casa di reclusione	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Autorizzazione all'esercizio dell'attività sanitaria (Dichiarazione Inizio Attività (DIA), comunicazione di inizio attività per privati, ecc.)	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali	
	.05	Igiene urbana, ambientale e sanità pubblica	Edilizia cimiteriale (aree di rispetto cimiteriale, pareri, osservazioni, regolamenti, ecc.)	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Pareri sanitari rilasciati agli Enti competenti in materia di scarichi, rifiuti, pozzi, ecc.	10 anni	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
3. Prevenzione medico - sanitaria	.06	Tutela salute attività sportive	Fascicolo accreditamento Centri Medicina dello Sport (domanda accreditamento, verbale sopralluogo, delibera accreditamento, prescrizioni)	ILLIMITATO	
	.06	Tutela salute attività sportive	Documenti relativi alla verifica attività sportive (verbale di accertamento, prescrizioni, ecc.)	ILLIMITATO	
	.06	Tutela salute attività sportive	Certificato medico di idoneità e inidoneità sportiva agonistica e non	5 anni	D.M. Sanità 18 febbraio 1982 ("Norme per la tutela sanitaria dell'attività sportiva agonistica")
	.06	Tutela salute attività sportive	Documentazione relativa alle pratiche di ricorso alla Commissione Regionale d'Appello contro il giudizio di non idoneità sportiva	ILLIMITATO	
	.07	Igiene degli alimenti	Autorizzazioni di attività di deposito/ vendita di prodotti fitosanitari;	5 anni dalla cessazione attività	
	.07	Igiene degli alimenti	Controllo e vigilanza sul deposito/ vendita ed utilizzo di prodotti fitosanitari	ILLIMITATO	
	.07	Igiene degli alimenti	Autorizzazioni sanitarie per locali e attrezzature per produzione, confezionamento, vendita e somministrazione di alimenti e bevande (es. copia Segnalazione Certificata di Inizio Attività - S.C.I.A. / Dichiarazione di Inizio Attività Produttiva - D.I.A.P.	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali	
	.07	Igiene degli alimenti	Pareri preventivi e tecnici per la realizzazione, attivazione o modifica di imprese alimentari	30 anni dalla cessazione attività	
	.07	Igiene degli alimenti	Certificazioni sanitarie per commercializzazione, esportazione ed importazione di prodotti alimentari	10 anni	
	.07	Igiene degli alimenti	Consulenza e controllo micologico	5 anni	
	.07	Igiene degli alimenti	Controllo e vigilanza sulla produzione, preparazione, confezionamento, deposito, trasporto, somministrazione e vendita di prodotti alimentari	ILLIMITATO	
	.07	Igiene degli alimenti	Campionatura alimenti e prodotti fitosanitari (verbale prelevamento campioni). Comprese richieste e certificato analisi. Verbal di controllo.	ILLIMITATO i verbali di controllo; 10 anni altra documentazione	
	.07	Igiene degli alimenti	Controllo sulle acque potabili destinate al consumo umano	ILLIMITATO i verbali di controllo; 10 anni altra documentazione (es. esiti)	
	.07	Igiene degli alimenti	Rilascio certificati di idoneità al consumo umano di acqua	5 anni	
	.07	Igiene degli alimenti	Procedimenti di sequestro a seguito di riscontro di non conformità alle normative sugli alimenti, sulla vendita deposito prodotti fitosanitari, sulle acque potabili destinate al consumo umano	ILLIMITATO	
	.07	Igiene degli alimenti	Interventi di polizia amministrativo/giudiziaria (es. vincoli, sequestri) nell'ambito dell'attività di controllo e vigilanza dei prodotti alimentari e prodotti fitosanitari	ILLIMITATO	
	.07	Igiene degli alimenti	Programmi di informazione-formazione abbinata all'igiene degli alimenti	10 anni; ILLIMITATO gli attestati; 1 anno attività informativa (compresi i questionari) con conservazione ILLIMITATA di un esemplare dépliant /manifesto / brochure	Si propone lo scarto di tutta l'attività istruttoria / interlocutoria relativa all'attività di formazione (cfr. I.4.13 conservazione di 5 per formazione personale dipendente e II.5.03 per MMG / PdF 10 anni). L'atto (decreto/determina) per iniziativa di formazione a conservazione ILLIMITATO Vengono conservati illimitatamente gli attestati e la brochure dell'iniziativa.
	.07	Igiene degli alimenti	Registro informativo tossinfezioni e malattie trasmissione alimentare	ILLIMITATO	
	.07	Igiene degli alimenti	Ispezioni e controlli acque minerali e termali	ILLIMITATO	
	.08	Igiene della nutrizione	Rilevamenti dello stato nutrizionale, dei consumi e delle abitudini nutrizionali per gruppi di popolazione (es. Registro sorveglianza nutrizionale scuole)	10 anni	
	.08	Igiene della nutrizione	Predisposizione, verifica e controllo delle tabelle dietetiche della ristorazione collettiva (es. Menù, segnalazione su menù, ecc.)	10 anni	
	.08	Igiene della nutrizione	Interventi di prevenzione nutrizionale per diffusione conoscenze di stili alimentari corretti e protettici	10 anni; 1 anno attività informativa (compresi i questionari) con conservazione ILLIMITATA di un esemplare dépliant / manifesto / brochure	Si tratta di campagne informative. Se le iniziative vengono formalizzate vengono assunti decreti/determine a conservazione illimitata. Viene conservata illimitatamente la brochure dell'iniziativa.
	.08	Igiene della nutrizione	Formazione / motivazione ad un corretto stile alimentare per gruppi di popolazione (counselling nutrizionale)	10 anni	Si tratta di campagne informative. Se le iniziative vengono formalizzate vengono assunti decreti/determine a conservazione illimitata. Viene conservata illimitatamente la brochure dell'iniziativa.
	.08	Igiene della nutrizione	Consulenze per il personale delle ristorazioni in tema nutrizionale	10 anni	
	.09	Laboratorio di prevenzione	Referti analisi campioni ufficiali (Rapporti di prova). Comprese le eventuali registrazioni (verbale prelievo, verbale di analisi, fogli di lavoro, stampate strumenti, risultati controlli di qualità, ecc.)	10 anni	
	.09	Laboratorio di prevenzione	Referti analisi campioni ed esami di laboratorio. Comprese le relative registrazioni (richiesta d'analisi, foglio di lavoro, liste analisi, schede pazienti per le indagini che prevedono risultati dei controlli di qualità, ecc.)	5 anni	nota regione Lombardia H1.2003.0001436

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Prevenzione veterinaria	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routinaria interna ed esterna attività di prevenzione veterinaria	5 anni	
	.02	Sanità animale	Rilascio pareri, autorizzazioni e nulla osta per attività / strutture oggetto di controllo e vigilanza Pareri per rilascio permessi di costruire insediamenti produttivi	10 anni	
	.02	Sanità animale	Rilascio attestazioni e certificazioni sanitarie previste da normative nazionali o regionali	10 anni	
	.02	Sanità animale	Interventi di profilassi delle malattie infettive degli animali	10 anni	
	.02	Sanità animale	Denunce malattie infettive e diffusive degli animali (zoonosi)	10 anni; ILLIMITATO i registri	
	.02	Sanità animale	Accertamenti diagnostici e campionamenti previsti da Piani Nazionali e/o Regionali su animali	10 anni	
	.02	Sanità animale	Controlli sanitari mirati a verificare l'eventuale presenza delle malattie degli animali (controlli diagnostici e di indagini sierologiche)	10 anni	
	.02	Sanità animale	Valutazione inconvenienti igienici connessi alla presenza di cani, gatti, piccioni, ecc.	10 anni	
	.02	Sanità animale	Ispezioni/controlli allevamenti e animali allevati	ILLIMITATO	
	.02	Sanità animale	Verbal di sopralluogo presso le strutture oggetto di vigilanza	ILLIMITATO	
	.02	Sanità animale	Indagini epidemiologiche a seguito di malattie infettive o casi sospetti	ILLIMITATO 10 anni per pratiche indennizzo	
	.02	Sanità animale	Interventi di polizia amministrativo/giudiziaria (es. vincoli, sequestri, dissequestri, prescrizioni) nell'ambito dell'attività di vigilanza	ILLIMITATO per verbali; 10 anni altra documentazione	
	.03	Anagrafe zootecnica e movimentazione animale	Rilascio certificazioni sanitarie / passaporti per la movimentazione	10 anni	
	.03	Anagrafe zootecnica e movimentazione animale	Dichiarazione di provenienza e destinazione degli animali (mod. IV)	3 anni	Unico riferimento normativo in vigore D.Lgs. 200/2010 relativo ai suini.
	.03	Anagrafe zootecnica e movimentazione animale	Controlli sanitari sugli animali introdotti da paesi comunitari ed extracomunitari	10 anni (salvo verbali di sequestro che ricadono nella voce precedente "Interventi polizia amm. / giudiziaria")	
	.03	Anagrafe zootecnica e movimentazione animale	Segnalazioni da ufficio veterinario adempimenti comunitari arrivi animali vivi e alimenti/mangimi	3 anni	In analogia con il termine del mod. IV
	.03	Anagrafe zootecnica e movimentazione animale	Gestione anagrafe animale (certificazioni, vidimazioni registri, Banca Dati Regionale, ecc.)	20 anni	
	.03	Anagrafe zootecnica e movimentazione animale	Assegnazione codici di stalla / Schede di stalla	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali	
	.03	Anagrafe zootecnica e movimentazione animale	Consistenza di stalla	10 anni	
	.03	Anagrafe zootecnica e movimentazione animale	Comunicazioni inerenti apiari (registrazione nuovi apiari, comunicazioni per apiari attivi, autorizzazioni per nomadismo...)	10 anni	
	.03	Anagrafe zootecnica e movimentazione animale	Passaporti capi macellati e deceduti in stalla	5 anni	Circolare DG Salute n. 11 del 13.03.2013 (per equini)
	.04	Igiene alimenti di origine animale	Rilascio autorizzazioni alla produzione / vendita di carni e derivati	10 anni <i>dalla cessazione attività</i>	
	.04	Igiene alimenti di origine animale	Rilascio pareri igienico-sanitari per l'attività di produzione, vendita e autotrasporto di carni e derivati	10 anni <i>dalla cessazione attività</i>	
	.04	Igiene alimenti di origine animale	Ispezioni / vigilanza / sopralluoghi stabilimenti produzione, lavorazione e deposito di carni e derivati	ILLIMITATO	
	.04	Igiene alimenti di origine animale	Certificazioni sanitarie spedizioni di carni e derivati (importazione / esportazione)	10 anni	
	.04	Igiene alimenti di origine animale	Rilascio pareri igienico-sanitari / idoneità / nulla osta per attività di macellazione animali negli stabilimenti e a domicilio	10 anni	
	.04	Igiene alimenti di origine animale	Documentazione relativa alle D.I.A. (Dichiarazioni Inizio Attività) / SCIA	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali	
	.04	Igiene alimenti di origine animale	Atti relativi e/o conseguenti agli interventi di polizia amministrativa/giudiziaria (es. vincoli, sequestri, ecc.)	ILLIMITATO	
	.04	Igiene alimenti di origine animale	Documentazione inerente la gestione degli stati di allerta - Relazione finale	ILLIMITATO	
	.04	Igiene alimenti di origine animale	Segnalazioni stati di allerta e conseguenti controlli per il ritiro dei prodotti	10 anni	
	.04	Igiene alimenti di origine animale	Campionamento per indagini microbiologiche e chimiche per la ricerca di residui pericolosi (ormoni, farmaci)	10 anni	
	.04	Igiene alimenti di origine animale	Rilascio autorizzazioni alla produzione/vendita dei prodotti della pesca, latte, uova, miele e loro derivati	10 anni <i>dalla cessazione attività</i>	
	.04	Igiene alimenti di origine animale	Rilascio pareri igienico-sanitari per l'attività di produzione/vendita/autotrasporto di prodotti della pesca, latte, uova, miele e loro derivati	10 anni <i>dalla cessazione attività</i>	
	.04	Igiene alimenti di origine animale	Vigilanza, tramite ispezioni e sopralluoghi, sui stabilimenti produzione, lavorazione e deposito alimenti di origine animale (prodotti della pesca, latte, uova, miele e loro derivati)	ILLIMITATO	
	.04	Igiene alimenti di origine animale	Rilascio certificazioni sanitarie per le spedizioni dei prodotti della pesca, latte, uova, miele e loro derivati	10 anni	
	.04	Igiene alimenti di origine animale	Campionamenti per indagini microbiologiche e chimiche per la ricerca di residui pericolosi (ormoni, farmaci) sui prodotti della pesca, latte, uova, miele e loro derivati	10 anni	
	.04	Igiene alimenti di origine animale	Indagine per sospetta tossi infezione alimentare a seguito di consumo di alimenti di origine animale	10 anni da ultima registrazione	
	.04	Igiene alimenti di origine animale	Analisi trichinella e altre analisi su capi macellati (esiti negativi)	1 anno	

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Prevenzione veterinaria	.05	Igiene allevamenti e produzioni zootecniche	Autorizzazioni e pareri igienico sanitari, nulla osta su allevamenti e le strutture zootecniche, automezzi e stabilimenti (es. mangimifici, produzione latte, acquicoltura, ambulatori, grossisti medicinali, farmacie)	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali	
	.05	Igiene allevamenti e produzioni zootecniche	Vigilanza e ai conseguenti provvedimenti su allevamenti e le strutture zootecniche, sugli automezzi e sugli stabilimenti oggetto di controllo (es. mangimifici, produzione latte, acquicoltura, ambulatori, grossisti medicinali, farmacie)	ILLIMITATO	
	.05	Igiene allevamenti e produzioni zootecniche	Gestione rapporti e rendicontazione con Agenzia per le Erogazioni in Agricoltura - AGEA	ILLIMITATO	
	.05	Igiene allevamenti e produzioni zootecniche	Autorizzazioni al trasporto degli animali	5 anni (se dati inseriti nella banca dati regionale delle anagrafi zootecniche)	
	.05	Igiene allevamenti e produzioni zootecniche	Attività di farmaco-vigilanza veterinaria (autorizzazioni, ispezioni)	ILLIMITATO	
	.05	Igiene allevamenti e produzioni zootecniche	Autorizzazioni alla scorta farmaci veterinari	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali o 2 anni dalla rinuncia all'autorizzazione	
	.05	Igiene allevamenti e produzioni zootecniche	Rilascio autorizzazioni alla riproduzione e fecondazione animale	10 anni	
	.05	Igiene allevamenti e produzioni zootecniche	Ispezioni e controlli sullo smaltimento dei rifiuti di origine animale	ILLIMITATO	
	.05	Igiene allevamenti e produzioni zootecniche	Attuazione dei piani nazionali e regionali di campionamento (PNR e PNAA)	ILLIMITATO in caso di non conformità campionamenti / rapporti di prova; 10 anni nei casi di conformità	
	.05	Igiene allevamenti e produzioni zootecniche	Campionamenti	10 anni	
	.05	Igiene allevamenti e produzioni zootecniche	Gestione degli stati di allerta nel settore della produzione zootecnica - Relazione finale	ILLIMITATO	
	.05	Igiene allevamenti e produzioni zootecniche	Segnalazioni stati di allerta e conseguenti controlli per il ritiro dei prodotti	10 anni	
	.05	Igiene allevamenti e produzioni zootecniche	Documenti relativi a interventi di formazione degli addetti in tema di benessere animale (allevamenti e trasporti)	10 anni	
	.05	Igiene allevamenti e produzioni zootecniche	Gestione farmaci veterinari (ricette)	5 anni	
	.05	Igiene allevamenti e produzioni zootecniche	Ispezioni / controlli sull'igiene delle produzioni animali da allevamento	ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Ispezioni e controlli sul benessere animale (visite ed esami)	ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Pratiche morsicature	10 anni	
	.06	Randagismo e tutela animali da affezione	Notifica vaccinazione antirabbica	10 anni; Registro ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Ispezioni/controlli sull'igiene delle produzioni animali da affezioni	ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Gestione del canile sanitario (registro carico-scarico, atti di cessione, ecc.)	10 anni	
	.06	Randagismo e tutela animali da affezione	Interventi sul territorio (richieste, programmazione, registrazione) / colonie feline	10 anni	
	.06	Randagismo e tutela animali da affezione	Rilascio certificazioni sanitarie	10 anni	
	.06	Randagismo e tutela animali da affezione	Ispezioni e sopralluoghi	ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Sterilizzazioni cani randagi e gatti appartenenti a colonie riconosciute	20 anni	Il termine di 20 anni è legato alla vita massima di un cane/gatto.
	.06	Randagismo e tutela animali da affezione	Gestione dell'anagrafe canina - Registro	ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Atti di trasferimento cani e documentazione correlata (compresi tatuaggi)	15 anni	
	.06	Randagismo e tutela animali da affezione	Schede / cartellini accalappiamento cani	15 anni	
	.06	Randagismo e tutela animali da affezione	Interventi contro il maltrattamento degli animali. Comprese segnalazioni e conseguenti provvedimenti	10 anni	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
5. Assistenza sanitaria	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routinaria interna ed esterna attività di assistenza sanitaria	5 anni	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria / routinaria interna ed esterna attività di assistenza sanitaria: appuntamenti per accertamento di idoneità e altri tipi di documentazione del genere	1 anno	
	.02	Emergenza sanitaria territoriale	Documentazione 118 compilata dalle équipes di soccorso dei MSB (Mezzi di Soccorso di Base, con soccorritori a bordo), dei MSI (Mezzi di Soccorso Intermedio, con infermiere a bordo) e dei MSA (Mezzi di Soccorso Avanzato, con medico e infermiere a bordo).	ILLIMITATO Conservazione da parte della Struttura ospedaliera di destinazione del paziente (in cartella clinica o quale parte integrante della documentazione di Pronto Soccorso)	
	.02	Emergenza sanitaria territoriale	Documentazione generata dall'applicativo gestionale di COEU (Centrale Operativa Emergenza Urgenza)/SOREU (Sala Operativa Regionale Emergenza Urgenza) e relativi allegati; registrazioni telefoniche intercorse tra la COEU (Centrale Operativa Emergenza Urgenza)/SOREU (Sala Operativa Regionale Emergenza Urgenza) e altri soggetti (utenti, équipes dei mezzi di soccorso, Forze di Polizia, ospedali, ecc.).	ILLIMITATO	
	.02	Emergenza sanitaria territoriale	Documentazione sanitaria utilizzata in occasione di maxi emergenze e di grandi eventi	30 anni	
	.02	Emergenza sanitaria territoriale	Trasferimento dei pazienti a bordo di mezzi di soccorso attrezzati	ILLIMITATO Conservazione da parte della Struttura ospedaliera di destinazione del paziente (in cartella clinica o quale parte integrante della documentazione di Pronto Soccorso)	
	.03	Assistenza sanitaria di base	Documentazione relativa alla gestione dei Medici di Medicina Generale - MMG e dei Pediatri di Famiglia - PdF (associazionismo medico, orari apertura, ecc.)	5 anni	
	.03	Assistenza sanitaria di base	Ricevute consegna ricettari	5 anni	Nota Regione Lombardia H1.2001.0033136 del 16/05//2001 Nota Regione Lombardia H1. 2005.0032866 del 05/07/2005 DM 17.03.2008 Le Matrici ricette compilate sono conservate a cura dei medici prescrittori per 5 anni
	.03	Assistenza sanitaria di base	Rendicontazione accessi Assistenza Domiciliare Integrata - ADI, Assistenza Domiciliare Programmata - ADP, Prestazioni di particolare Impegno Professionale - PIP, prestazioni erogate per adesione a progetti / iniziative e documentazione su competenze economiche dei Medici di medicina generale - MMG e Pediatri di Famiglia - PdF	5 anni	
	.03	Assistenza sanitaria di base	Cartelle e fascicoli relativi all'assistenza domiciliare	5 anni dal termine dell'assistenza	
	.03	Assistenza sanitaria di base	Controllo / sopralluogo studi Medici di Medicina Generale - MMG e Pediatri di Famiglia - PdF ed eventuali prescrizioni	ILLIMITATO	
	.03	Assistenza sanitaria di base	Controllo e valutazione assistenza erogata dai Medici di Medicina Generale - MMG e dai Pediatri di Famiglia - PdF (es. vaccinazioni, ADI, ADP, screening, assistenza farmaceutica)	10 anni	
	.03	Assistenza sanitaria di base	Formazione dei Medici di Medicina Generale - MMG e dei Pediatri di Famiglia - PdF	10 anni	
	.03	Assistenza sanitaria di base	Documentazione su scelta / revoca dei Medici di Medicina Generale - MMG e dei Pediatri di Famiglia - PdF (Iscrizione al SSR, domande autorizzazione, cambio, variazioni anagrafiche, ecc.)	5 anni. 1 anno se esiste l'anagrafe informatizzata degli assistiti 5 anni comunque per stranieri	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
5. Assistenza sanitaria	.03	Assistenza sanitaria di base	Ambiti carenti per la Medicina Generale, la Pediatria di Famiglia e di Continuità Assistenziale e relative coperture (richieste conferimento, assegnazione e accettazioni dei medici, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Documentazione per riconoscimento diritto all'esenzione (copia cartella clinica, verbale invalidità, certificati medici, archivio esenti, ecc.)	5 anni	
	.03	Assistenza sanitaria di base	Autocertificazioni per esenzioni da ticket sanitario	10 anni	In ragione della prescrizione decennale del diritto di credito al recupero ticket (art. 2946 c.c.)
	.03	Assistenza sanitaria di base	Documentazione relativa alla gestione dei medici di Continuità Assistenziale (avvisi, graduatorie, incarichi, ecc.)	ILLIMITATO	
	.03	Assistenza sanitaria di base	Documentazione relativa alla attività di Continuità Assistenziale (registro interventi, referti delle visite ecc.)	ILLIMITATO i Registri, 10 anni altra documentazione	
	.03	Assistenza sanitaria di base	Controllo e valutazione assistenza erogata dai medici di Continuità Assistenziale	10 anni	
	.03	Assistenza sanitaria di base	Documentazione relativa a Strutture per cure sub acute (consenso al trasferimento paziente, scheda sanitaria pazienti, documentazione trasferimento, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Documentazione relativa alla presa in carico del paziente cronico e/o fragile (Piano di Assistenza Individuale - PAI, patto di cura, ecc.). Documentazione relativa al Cronic Related Group - CReG.	10 anni dall'ultima registrazione	
	.03	Assistenza sanitaria di base	Documentazione prodotta per rimborsi assistenza indiretta in Italia (documentazione di spesa originale e quietanzata, copia cartelle cliniche, dichiarazione non convenzione con il SSN, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Documentazione prodotta per rimborsi cure all'estero (valutazione centri regionali di riferimento, fatture, copia cartelle cliniche, liquidazione, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Documentazione relativa a stranieri (Dichiarazione indigenza, tessera sanitaria STP e registro codici STP, richiesta rimborso ricovero alla Prefettura, iscrizione volontaria SSR, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Modelli esteri comunitari	10 anni	
	.03	Assistenza sanitaria di base	Assistenza all'estero (modelli esteri Paesi in convenzione bilaterale, AIRE, documentazione ex DPR 618/1980, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Rimborsi dializzati	10 anni	
	.03	Assistenza sanitaria di base	Gestione funzionalità tessera sanitaria (richieste duplicati, richiesta PIN / GASS, ecc.)	1 anno	
	.03	Assistenza sanitaria di base	Concessione forniture extra prontuario	5 anni dal decesso o dalla cessazione per fascicolo assistito 5 anni per verbali commissione ILLIMITATO per atto di concessione	
	.04	Assistenza protesica e integrativa	Documentazione relativa all'erogazione dei dispositivi medici, di protesi, ortesi, presidi, ausili e prodotti dietetici, presidi per diabetici (domanda, certificato attestante la patologia, prescrizione specialistica, Progetto riabilitativo individuale e/o piano terapeutico, copia verbale invalidità, ricevuta consegna, ecc.) e relativa autorizzazione.	1 anno dalla data del decesso o dal termine dell'erogazione	
	.04	Assistenza protesica e integrativa	Documentazione attestante la fornitura dei dispositivi medici, dei presidi e dei prodotti dietetici	5 anni	
	.04	Assistenza protesica e integrativa	Rendiconto periodico da parte delle farmacie per forniture indirette prodotti dietetici	5 anni	
	.04	Assistenza protesica e integrativa	Autorizzazione / Fornitura per pazienti ipossiemicici	1 anno dalla data del decesso o dal termine dell'erogazione	
	.04	Assistenza protesica e integrativa	Documentazione inerente la valutazione e il controllo dell'assistenza integrativa erogata	10 anni	
	.04	Assistenza protesica e integrativa	Report dati relativo agli utenti e ai prescrittori per la fornitura protesi, ortesi ed ausili, dispositivi medici, presidi e prodotti dietetici, presidi per diabetici	5 anni	
	.04	Assistenza protesica e integrativa	Documentazione relativa a gestione magazzino protesi, ortesi ed ausili (atti preparatori alla gara d'appalto, ordini dei dispositivi di gara, bolle di consegna / ritiro ausili al domicilio dell'assistito)	5 anni	
	.05	Assistenza psichiatrica e neuropsichiatrica infantile	Cartella clinica di struttura semiresidenziale, Centro Diurno e Residenzialità Leggera. Documentazione relativa alla neuropsichiatria dell'infanzia e dell'adolescenza.	10 anni	
	.05	Assistenza psichiatrica e neuropsichiatrica infantile	Cartella clinica di struttura residenziale (diario clinico, visite psichiatriche, attività riabilitative, colloqui psicoterapeutici, ecc.). Documentazione relativa alla neuropsichiatria dell'infanzia e dell'adolescenza	ILLIMITATO	
	.05	Assistenza psichiatrica e neuropsichiatrica infantile	Documentazione del sistema informatizzato regionale PSICHE	Secondo tipologia di regime di erogazione della prestazione (residenziale / semiresidenziale)	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
6. Assistenza socio - sanitaria integrata	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione e pianificazione delle unità di offerta sociosanitarie (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routine interna ed esterna attività di assistenza socio sanitaria integrata	5 anni	
	.01	Aspetti generali, organizzativi e gestionali	Progetti sociosanitari (atti di approvazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria relativa a progetti.	10 anni	
	.02	Dipendenze	Accertamento dipendenza su richiesta di aziende (elenco soggetti sottoposti ad accertamento, esito accertamenti, referti esami di laboratorio, documentazione varia, ecc.)	ILLIMITATO in cartella sanitaria. 1 anno altri esemplari	D.P.C.M. 10.2.84; DPR 14 gennaio 1997
	.02	Dipendenze	Cartella sanitaria SERT (Cartella SESIT con percorso di cura, dati clinici, esami laboratorio, visite, consensi, piani terapeutici, ecc.)	ILLIMITATO	
	.02	Dipendenze	Adempimenti connessi agli inserimenti in comunità terapeutiche di alcolisti e tossicodipendenti (certificati tossicodipendenza, ecc.)	10 anni	
	.02	Dipendenze	Richieste di certificazione dello stato di tossicodipendenza	ILLIMITATO	
	.02	Dipendenze	Flussi informativi del SERT (Flussi regionali, Report di attività e per la remunerazione, ecc.)	10 anni. ILLIMITATO se allegate a delibere o a documenti di programmazione	Decr. Leg. 29/98 e successive modifiche ed integrazioni
	.02	Dipendenze	Comunicazione tra strutture per trasferimento di tossicodipendenti (pazienti "appoggiati")	10 anni	
	.02	Dipendenze	Procedimenti per utenti segnalati dagli uffici territoriali del governo (richieste di intervento / valutazione, convocazione, foglio firma presenze, relazioni, comunicazioni, decreti, ecc.)	ILLIMITATO	
	.02	Dipendenze	Segnalazioni dagli uffici territoriali del governo e altri enti/istituzioni senza seguito	10 anni	
	.02	Dipendenze	Adempimenti inerenti alle misure alternative alla detenzione	ILLIMITATO	
	.02	Dipendenze	Richieste di consulenza su dipendenza da parte dei reparti ospedalieri, MMG, familiari, ecc.	10 anni	
	.02	Dipendenze	Progetti su dipendenze (<i>compresi gli</i> atti di approvazione)	ILLIMITATO	
	.02	Dipendenze	Attività formativa su dipendenze	10 anni	
	.02	Dipendenze	Attività informativa (compresi i questionari)	1 anno con conservazione ILLIMITATA per un esemplare dell'iniziativa/manifesto/brochure	Si tratta di campagne informative. Se le iniziative vengono formalizzate vengono assunti decreti/determine a conservazione illimitata. Viene conservata illimitatamente la brochure dell'iniziativa.
	.02	Dipendenze	Documentazione istruttoria e corrispondenza relativa ad interventi di prevenzione su dipendenze	10 anni	
	.02	Dipendenze	Cartella sanitaria Alcolologia - NOA (Documentazione sanitaria, consulti psicologici, valutazioni sociali, comprendenti anche documentazione con dati riguardanti i familiari, consensi informati, informazioni inerenti i ricoveri, dati clinici, esami laboratorio, visite, ecc.)	ILLIMITATO	
	.03	Famiglia, infanzia ed età evolutiva	Fascicolo socio-sanitario utente del Consultorio Familiare (Documentazione sanitaria, consulti psicologici, valutazioni sociali, comprendenti anche documentazione con dati riguardanti i familiari, consensi informati, informazioni inerenti i ricoveri, referti, valutazioni cliniche e psicologiche, schede, questionari, documenti contenenti dati sanitari, copia certificazione per IVG, ecc.)	20 anni	
	.03	Famiglia, infanzia ed età evolutiva	Documentazione relativa a minori sottoposti all'autorità giudiziaria (Adozioni, affidi, abbandoni, maltrattamenti, abusi, interventi di sostegno, vicende giudiziarie, ecc.)	ILLIMITATO	
	.03	Famiglia, infanzia ed età evolutiva	Segnalazione donne vittima di violenza	20 anni	
	.03	Famiglia, infanzia ed età evolutiva	Documentazione relativa a minori non riconosciuti	ILLIMITATO	
	.03	Famiglia, infanzia ed età evolutiva	Richieste dell'autorità giudiziaria assistenza psicologica per audizioni protette minori	5 anni	
	.03	Famiglia, infanzia ed età evolutiva	Segnalazione da ospedale per dimissioni protette post partum	1 anno	
	.03	Famiglia, infanzia ed età evolutiva	Documentazione relativa a gruppi consultoriali (allattamento, pre parto, contraccezione, menopausa, ecc.): scheda iscrizione, consenso al trattamento dati, foglio presenza, ecc.	1 anno	

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
6. Assistenza socio - sanitaria integrata	.04	Assistenza domiciliare	Documentazione relativa all'erogazione di contributi economici a favore delle famiglie che assistono in casa persone non autosufficienti	10 anni	
	.04	Assistenza domiciliare	Documentazione inerente l' erogazione di assistenza domiciliare (Assegnazione del credit o voucher socio-sanitario, autorizzazione, Piani individuali di assistenza, attivazione, cartella socio-sanitaria utenti , verbali di equipe valutazione multidimensionale, ecc.)	5 anni <i>dal termine dell'assistenza</i>	
	.04	Assistenza domiciliare	Controllo e valutazione assistenza domiciliare erogata (verbali di controllo ed eventuali prescrizioni, report dei controlli)	ILLIMITATO	
	.04	Assistenza domiciliare	Autorizzazione erogazione ADI per utenti extra regione	5 anni	
	.04	Assistenza domiciliare	Segnalazioni per ingresso cure palliative (hospice)	1 anno	
	.04	Assistenza domiciliare	Segnalazioni di valutazione multidimensionale non attivate	1 anno	
	.05	Disabilità	Documenti prodotti nell'ambito di programmi e progetti anche di vita indipendente del disabile	10 anni	
	.05	Disabilità	Interventi personalizzati di valutazione delle capacità, analisi delle mansioni, orientamento e successivo inserimento in contesto lavorativo (compresi i certificati di svantaggio)	10 anni dall'ultima registrazione	
	.05	Disabilità	Procedimento relativo all'inserimento di alunni disabili nel contesto scolastico (istanze, convocazioni accertamento collegiale, documentazione sanitaria, verbale di accertamento, certificazioni , ecc.)	10 anni dall'ultima registrazione	
	.05	Disabilità	Concessione di contributi economici alle famiglie	10 anni	
	.05	Disabilità	Richiesta contributi per le spese ai sensi dell'art. 27 della legge 104 (richieste, valutazione, autorizzazione, documentazione sanitaria allegata)	10 anni	
	.06	Fragilità	Documentazione in strutture residenziali o semiresidenziali sociosanitarie (Domande inserimento, autorizzazioni, schede ingresso e dimissioni, valutazione socio-sanitaria, piano di assistenza personalizzato, copie di documentazione sanitaria, ecc.)	10 anni	
	.06	Fragilità	Documentazione monitoraggio delle strutture residenziali e semiresidenziali	10 anni	
	.06	Fragilità	Flussi informativi (Scheda di Osservazione Intermedia Assistenza - SOSIA, Scheda Individuale Disabile - SIDI, Scheda Riabilitazione - RIA, ecc.	10 anni. ILLIMITATO se allegate a delibere o a documenti di programmazione	
	.06	Fragilità	Verbali di equipe per valutazione multidimensionale	5 anni dall'ultima registrazione	
	.06	Fragilità	Fascicolo Socio Assistenziale e Sanitario (FaSaS) (cartella utente)	10 anni dall'ultima registrazione	
	.06	Fragilità	Documentazione relativa all'amministrazione di sostegno, tutele e curatele	ILLIMITATO	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
7. Governo sanitario e sociosanitario	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione e pianificazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routine interna ed esterna attività di governo sanitario e sociosanitario	5 anni	
	.02	Osservatorio epidemiologico	Indagini e statistiche demografiche ed epidemiologiche	10 anni ILLIMITATO se allegate a delibere o a documenti di programmazione	
	.03	Flussi informativi sanitari e sociosanitari	Flussi informativi Ministeriali, Regionali, altri enti	10 anni. ILLIMITATO se allegate a delibere o a documenti di programmazione	Decr. Leg. 29/98 e successive modifiche ed integrazioni
	.04	Accreditamento e controllo strutture sanitarie	Documentazione relative a istanze di accreditamento / autorizzazioni / ampliamento (requisiti, planimetrie, procedure dell'ente, delibere di accreditamento, dichiarazioni di conformità, elenchi personale, ecc.)	ILLIMITATO	
	.04	Accreditamento e controllo strutture sanitarie	Documentazione relative a vigilanza / controllo accreditamento (segnalazioni, autocertificazioni, verbale di controllo e sanzionatorio, provvedimenti di sospensione / revoca, perizie asseverate, ecc.)	ILLIMITATO	
	.04	Accreditamento e controllo strutture sanitarie	Autocertificazioni periodiche sulla dotazione organica	5 anni	
	.05	Autorizzazione e controllo strutture sociosanitarie	Documentazione relative a istanze di accreditamento / autorizzazioni / ampliamento (requisiti, planimetrie, procedure dell'ente, delibere di accreditamento, dichiarazioni di conformità, elenchi personale, ecc.).	ILLIMITATO	
	.05	Autorizzazione e controllo strutture sociosanitarie	Documentazione relative a vigilanza / controllo accreditamento (segnalazioni, autocertificazioni, verbale di controllo, provvedimenti di sospensione / revoca, perizie asseverate, ecc.)	ILLIMITATO	
	.06	Acquisto e controllo prestazioni sanitarie	Documentazione relativa alle attività dei controlli sulle prestazioni (moduli di registrazione, campionamento e programmazione, copie cartelle e documentazione sanitaria, comunicazioni, ecc.)	10 anni	
	.06	Acquisto e controllo prestazioni sanitarie	Documentazione relativa agli esiti dei controlli sui ricoveri (Verbale di controllo e sanzionatorio, controdeduzioni, denunce / esposti / segnalazioni)	ILLIMITATO	
	.06	Acquisto e controllo prestazioni sanitarie	Documentazione relativa agli esiti dei controlli sulle prestazioni ambulatoriali (Verbale di controllo e sanzionatorio, controdeduzioni, denunce / esposti / segnalazioni)	ILLIMITATO	
	.06	Acquisto e controllo prestazioni sanitarie	Attività di autorizzazione, inserimento, proroga, trasferimento di pazienti psichiatrici in strutture residenziali e semiresidenziali (richieste, autorizzazioni, documentazione allegata)	10 anni	
	.06	Acquisto e controllo prestazioni sanitarie	Verballi di sopralluogo presso le strutture residenziali e semiresidenziali in ambito salute mentale	ILLIMITATO	
	.06	Acquisto e controllo prestazioni sanitarie	Contratti con strutture sanitarie	ILLIMITATO	
	.06	Acquisto e controllo prestazioni sanitarie	Documentazione relativa alle rendicontazione delle attività delle strutture sanitarie	10 anni	
	.07	Acquisto e controllo prestazioni sociosanitarie	Documentazione relativa alle attività dei controlli sulle prestazioni (moduli di registrazione, campionamento e programmazione, copie cartelle e documentazione sanitaria, comunicazioni, ecc.)	10 anni	
	.07	Acquisto e controllo prestazioni sociosanitarie	Documentazione relativa agli esiti dei controlli sui ricoveri (Verbale di controllo e sanzionatorio, controdeduzioni, denunce / esposti / segnalazioni)	ILLIMITATO	
	.07	Acquisto e controllo prestazioni sociosanitarie	Documentazione relativa agli esiti dei controlli sulle prestazioni (Verbale di controllo e sanzionatorio, controdeduzioni, denunce / esposti / segnalazioni)	ILLIMITATO	
	.07	Acquisto e controllo prestazioni sociosanitarie	Contratti con strutture ed enti gestori socio-sanitari	ILLIMITATO	
	.07	Acquisto e controllo prestazioni sociosanitarie	Documentazione relativa alle rendicontazione delle attività delle unità d'offerta sociosanitarie (RSA, RSD, Cure Domiciliari, ecc.)	10 anni	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
8. Medicina legale	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routine interna ed esterna attività di medicina legale	5 anni	
	.02	Attività medico-legale e necroscopica	Soggiorni climatici ex ONIG / invalidi di guerra e di servizio (richiesta autorizzazione, documentazione sanitaria, autorizzazione, richiesta rimborso e conseguente liquidazione)	10 anni dall'ultima autorizzazione	
	.02	Attività medico-legale e necroscopica	Accertamenti sanitari su lavoratori visite fiscali (richieste e referti)	5 anni se non in fascicolo personale	
	.02	Attività medico-legale e necroscopica	Documenti riguardanti visite collegiali di idoneità / inidoneità alla mansione lavorativa compresi atti (certificato medico, documentazione sanitaria, ecc.)	20 anni	
	.02	Attività medico-legale e necroscopica	Accertamento medico e domanda in merito all'interdizione dal lavoro delle lavoratrici in stato di gravidanza	5 anni	Decreto Legislativo 26 marzo 2001, n.151.
	.02	Attività medico-legale e necroscopica	Consulenza medico legale in tema di riconoscimento della dipendenza da causa di servizio	20 anni	
	.02	Attività medico-legale e necroscopica	Documentazione per accertamenti decessi (certificati necroscopici)	ILLIMITATO	
	.02	Attività medico-legale e necroscopica	Documentazione per rilascio / rinnovo delle patenti di guida in caso di malattie o minorazioni anatomiche o funzionali rilasciate dalla Commissione Medica Locale (certificazione sanitaria, dichiarazione precedenti morbosità, certificato anamnestico, ecc.)	10 anni dalla visita	Armonizzazione con i tempi di conservazione di altri enti sanitari
	.02	Attività medico-legale e necroscopica	Contabilità (atti di liquidazione componenti commissione medica e documentazione corredata)	10 anni	
	.02	Attività medico-legale e necroscopica	Giudizio di idoneità patente di guida e nautica, pratiche per il rilascio e rinnovo (compreso originale ricevuta versamento diritti e certificato anamnestico)	1 anno	Decreto Ministero delle Infrastrutture e dei Trasporti n. 182 del 2 agosto 2016 (Note all'art. 3 di cui all'art. 36 c.3 del decreto ministeriale 29 luglio 2008, n. 146)
	.02	Attività medico-legale e necroscopica	Documentazione per rilascio / rinnovo del porto d'armi, compresa la documentazione sanitaria acquisita dal paziente	5 anni	
	.02	Attività medico-legale e necroscopica	Atti contenuti nel fascicolo relativo all'accertamento medico legale, compresa la documentazione inerente i rapporti e i flussi informativi con enti esterni	ILLIMITATO	
	.02	Attività medico-legale e necroscopica	Richieste e referti di visita medico-legale	20 anni	
	.03	Invalità civile, sordomutismo e menomazioni visive	Documentazione per riconoscimento o aggravamento stati invalidità civile, cecità e sordità, handicap e diritto al lavoro disabili (istanze di riconoscimento, certificato medico attestante la patologia invalidante, documentazione sanitaria, verbale di accertamento, verbale INPS, verbale handicap, ecc.).	ILLIMITATO	
	.03	Invalità civile, sordomutismo e menomazioni visive	Documentazione per rilascio / rinnovo del contrassegno invalidi, compresa la documentazione acquisita dal paziente	5 anni	
	.04	Istanze di indennizzo	Documentazione relativa ai danneggiati da vaccinazioni obbligatorie: pratiche di indennizzo (copie conformi di: certificato vaccinale, cartella clinica, documentazione sanitaria comprovante l'entità delle lesioni, documentazione amministrativa, ecc.)	ILLIMITATO	art.3 L.210/1992 e L. 238/1997); Circ. 1 Ministero della sanità del 4-11-1996 n. 900
	.04	Istanze di indennizzo	Documentazione relativa ai danneggiati da trasfusione o somministrazione di emoderivati: pratiche di indennizzo (copie conformi di: cartella clinica riportante la prova delle avvenute trasfusioni o somministrazioni emoderivati, documentazione sanitaria indicante positività o diagnosi di malattia, analisi ematochimiche, documentazione amministrativa, ecc.)	ILLIMITATO	art.3 L.210/1992 e L. 238/1997); Circ. 1 Ministero della sanità del 4-11-1996 n. 900

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04 TITOLO 2 - Area Sanitaria e Sociosanitaria territoriale					
CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
9. Assistenza e governo farmaceutica	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione, regolamentazione dei rapporti tra il Servizio Sanitario Nazionale e le farmacie).	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routinaria interna ed esterna attività assistenza e governo farmaceutica	5 anni	
	.01	Aspetti generali, organizzativi e gestionali	Gestione ricettari SSN (gestione ordini, rendicontazioni, consegna / registrazione ricettari MMG, PdF, MCA, RSA e strutture ospedaliere)	5 anni	
	.02	Controllo spesa farmaceutica	Monitoraggio / Report sul consumo / impiego di farmaci	5 anni	
	.02	Controllo spesa farmaceutica	Analisi sul consumo delle risorse per farmaci SSN da parte dei MMG, PdF, medici continuità assistenziale e specialisti ospedalieri	5 anni	
	.02	Controllo spesa farmaceutica	Analisi sul consumo delle risorse per farmaci di fascia H erogati in regime di file F	5 anni	
	.02	Controllo spesa farmaceutica	Verbale di controllo / sopralluogo file F	ILLIMITATO	
	.02	Controllo spesa farmaceutica	Analisi sulla corretta erogazione e pagamento di ricette di farmaci in regime di SSN	5 anni (in assenza di contenziosi)	
	.02	Controllo spesa farmaceutica	Contenzioso con Farmacie relativo a ricette contestate (verbale controllo, sanzionatorio, segnalazione autorità giudiziaria, ecc.)	ILLIMITATO	
	.02	Controllo spesa farmaceutica	Documenti relativi a interventi da parte dei NAS di richiesta di informazioni sulle modalità di prescrizione dei farmaci	ILLIMITATO	
	.03	Controllo farmacie, parafarmacie e distributori	Visita ispettiva ordinaria/straordinaria presso le farmacie (Verbale di controllo / sopralluogo, notifiche, ecc.)	ILLIMITATO	
	.03	Controllo farmacie, parafarmacie e distributori	Visita ispettiva sui depositi e magazzini all'ingrosso di medicinali	ILLIMITATO	
	.04	Autorizzazione e governo farmacie	Autorizzazione all'apertura di esercizio farmaceutico (richieste, autorizzazioni, decadenza autorizzazione, ecc.)	ILLIMITATO (sino alla cessazione dell'attività o modifiche alla titolarità dell'esercizio – subingressi)	
	.04	Autorizzazione e governo farmacie	Regolamentazione in ordine alla fissazione di orari, turni, ferie ecc. delle farmacie	ILLIMITATO (sino alla cessazione dell'attività o modifiche alla titolarità dell'esercizio – subingressi)	
	.04	Autorizzazione e governo farmacie	Tenuta del registro dei farmacisti (nuove assunzioni, cessazioni, stati di servizio, nomina titolari e sostituti, ecc.)	ILLIMITATO (sino alla cessazione dell'attività o modifiche alla titolarità dell'esercizio – subingressi)	
	.04	Autorizzazione e governo farmacie	Richiesta e autorizzazioni di modifiche dei locali	ILLIMITATO (sino alla cessazione dell'attività o modifiche alla titolarità dell'esercizio – subingressi)	
	.04	Autorizzazione e governo farmacie	Richiesta e autorizzazioni trasferimento farmacie	ILLIMITATO (sino alla cessazione dell'attività o modifiche alla titolarità dell'esercizio – subingressi)	
	.05	Farmacovigilanza	Utilizzo farmaci fuori dalle prescrizioni (off-label)	10 anni	
	.05	Farmacovigilanza	Indicazioni/attività in applicazione di note AIFA (comprese comunicazioni di sicurezza d'uso)	10 anni	
	.05	Farmacovigilanza	Scheda di segnalazione di sospetta reazione avversa e le relative richieste di registrazione nel sito della farmacovigilanza del Ministero della Salute	ILLIMITATO	
	.05	Farmacovigilanza	Documenti relativi a ritiri o revoche di medicinali così come gli interventi di prelievo di farmaci ritenuti difettosi	5 anni	
	.05	Farmacovigilanza	Attività di vigilanza effettuate presso ospedali o altre strutture relative a gestione farmaci (medicinali scaduti, giacenza farmaci, pulizia armadi, disposizione farmaci, grado di umidità, luce, temperatura, recipienti a norma, correttezza gas medicinali, ecc.)	ILLIMITATO	
	.06	Assistenza farmaceutica diretta	Documenti relativi a garantire la fornitura di dispositivi medici (DM), presidi, farmaci e dietetici tramite dispensazione diretta (Richiesta autorizzazione ed erogazione diretta trattamenti e farmaci, ordine farmaci, registro smaltimento farmaci, ecc.)	5 anni	
	.07	Sperimentazione farmaci e dispositivi	Documenti che riguardano la sperimentazione di nuovi farmaci o l'uso di farmaci conosciuti al fine di verificarne l'effetto (Proposte di sperimentazioni, pareri del Comitato Etico, sottoscrizioni dei protocolli di studio, autorizzazione sperimentazione, ecc.)	25 anni (si veda anche cod. 3.11.00)	L'art. 58, comma 1 del regolamento EU 536/14 sulla sperimentazione dei medicinali sull'uomo, dispone quanto segue: A meno che il diritto dell'Unione preveda un periodo di archiviazione maggiore, il promotore e lo sperimentatore conservano il contenuto del fascicolo permanente della sperimentazione clinica per almeno venticinque anni dalla conclusione della medesima. Tuttavia, le cartelle cliniche dei soggetti sono archiviate in conformità del diritto nazionale.
	.08	Gestione stupefacenti	Documenti che riguardano gli stupefacenti (tenuta e distribuzione dei ricettari, monitoraggio sul quantitativo di stupefacenti erogato dalle farmacie o strutture convenzionate, ecc.)	5 anni	
	.08	Gestione stupefacenti	Registri di entrata e uscita degli stupefacenti	10 anni dalla data dell'ultima registrazione per enti e imprese autorizzati alla fabbricazione 5 anni dalla data dell'ultima registrazione per le officine autorizzate all'impiego e per le imprese autorizzate al commercio all'ingrosso 2 anni dalla data dell'ultima registrazione per le farmacie aperte al pubblico e le farmacie ospedaliere	DPR n.390/90 art. 60 e s.i.m. comma 1 Nota Regione Lombardia H1.2014.0019108 del 27.05.2014 Legge n. 38 del 15.03.2010 art. 10
	.08	Gestione stupefacenti	Registri di carico e scarico degli stupefacenti (registro delle unità operative)	2 anni dalla data dell'ultima registrazione	DPR n.390/90 art. 60 e s.i.m. comma 3 e 6 Nota Regione Lombardia H1.2014.0019108 del 27.05.2014 Legge n. 38 del 15.03.2010 art. 10
	.08	Gestione stupefacenti	Buoni / ordini di acquisto stupefacenti e documenti trasporto / fatture	10 anni	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 3 - Area Ospedaliera

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
1. Direzione ospedaliera	.01	Aspetti generali, organizzativi e gestionali	Contestazioni anomalie SDO	10 anni	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione pagamenti ad altre strutture ospedaliere	5 anni	
	.01	Aspetti generali, organizzativi e gestionali	Pagamento ticket, ricevute	5 anni	Nota Regione Lombardia H1.2003.0001436. Allegato 3 alla DGRV1118178 del 18.02.2002
	.01	Aspetti generali, organizzativi e gestionali	Pratiche amministrative per ricoveri (stranieri, comunitari, solventi)	10 anni	
	.01	Aspetti generali, organizzativi e gestionali	Appropriatezza ricoveri (PRUO, ecc.)	10 anni	
	.01	Aspetti generali, organizzativi e gestionali	Volontariato, registri	10 anni	
	.01	Aspetti generali, organizzativi e gestionali	Registri viaggi ambulanza per trasferimento pazienti per esami in altre strutture; Autorizzazione trasporti in ambulanza	1 anno	
	.01	Aspetti generali, organizzativi e gestionali	Richieste copie di cartelle cliniche ed ambulatoriali, schede di P.S., certificati di ricovero, referto esami di laboratorio, ecc.	1 anno	
	.01	Aspetti generali, organizzativi e gestionali	Deleghe per il ritiro dei referti / cartelle cliniche	1 anno	
	.01	Aspetti generali, organizzativi e gestionali	Reclami	10 anni	
	.01	Aspetti generali, organizzativi e gestionali	CUP, prenotazione per prestazioni	1 anno	
	.01	Aspetti generali, organizzativi e gestionali	Gestioni reti di patologia (adesione e organizzazione), i dati relativi alle singole prestazioni di cura saranno classificati negli appositi sistemi gestionali	ILLIMITATO per la documentazione organizzativa; per la documentazione relativa ai sistemi gestionali si fa riferimento alla tipologia di assetto assistenziale erogato (prestazione ambulatoriale, ricovero)	
	.01	Aspetti generali, organizzativi e gestionali	Registrazioni audio, Videoregistrazioni, Fotografie digitali / analogiche relative a prestazioni sanitarie	Tempo di conservazione correlato al documento principale, massimo 10 anni.	
	.01	Aspetti generali, organizzativi e gestionali	Registrazioni informatiche di monitoraggio di parametri biologici (es. ECG, EEG, ecc.)	Tempo di conservazione correlato al documento principale, massimo 10 anni.	
	.02	Rapporti con l'autorità giudiziaria	Documentazione relativa a segnalazioni / denunce all'Autorità Giudiziaria	ILLIMITATO	
	.03	Igiene ospedaliera	Documentazione relativa ai controlli della sterilizzazione (prove Bowie Dick, Grafici dei cicli-rintracciabilità); modulistica carico/scarico strumentario, richieste dei reparti e documentazione della sterilizzazione in genere	2 anni	
	.03	Igiene ospedaliera	Registri ossido di etilene	2 anni	
	.03	Igiene ospedaliera	Inchieste o indagini epidemiologiche su malattie infettive di particolare rilevanza e/o soggette a sorveglianza	10 anni	Circ. Min. Sanità n. 61 del 19/12/1986. In considerazione del termine di prescrizione del diritto al risarcimento del danno subito da un paziente che è di dieci anni, siffatta documentazione verrà conservata sino al compimento della prescrizione decennale. Ministero per i Beni culturali e per le attività culturali -Direzione Generale per gli Archivi (prontuario scarto ASL)
	.03	Igiene ospedaliera	Malattie infettive, registri	ILLIMITATO	
	.03	Igiene ospedaliera	Registro carico e scarico rifiuti speciali, integrati con i formulari relativi al trasporto dei rifiuti	5 anni dalla data dell'ultima registrazione	D.Lgs. n.22/97 art.12 e s.m.i. (art. 190 del D.Lgs. n.152/2006 come modificato dalla legge 125/2013)
	.03	Igiene ospedaliera	Controlli microbiologici ambientali (schede, relazioni, verbali, conclusioni, comunicazioni)	5 anni	In considerazione del termine di prescrizione del diritto al risarcimento del danno subito da un paziente che è di dieci anni, siffatta documentazione verrà conservata sino al compimento della prescrizione decennale.
	.03	Igiene ospedaliera	Vaccinazioni, campagne vaccinali: danni da vaccini	ILLIMITATO	
	.04	Radioprotezione	Valutazioni di sorveglianza ambientale e valutazioni della dose ricevuta od impegnata dai lavoratori esposti non classificati in categoria A, nonché i verbali di controllo dei dispositivi e degli strumenti di protezione di cui allo stesso articolo.	5 anni dalla data di compilazione	D.Lgs. n.230/1995 (art.81, c.3)
	.04	Radioprotezione	Schede personali sulle quali devono essere annotati i risultati delle valutazioni delle dosi individuali e delle introduzioni individuali; relazioni sulle circostanze ed i motivi inerenti alle esposizioni accidentali di emergenza nonché alle altre modalità di esposizione.	Sino alla cessazione del rapporto di lavoro mantenendone successivamente copia per almeno cinque anni	D.Lgs. n.230/1995 (art.81, c.3)
	.04	Radioprotezione	Risultati delle misurazioni di sorveglianza fisica della radioprotezione	10 anni	D.Lgs. n.230/1995 (art.81, c.3)

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 3 - Area Ospedaliera

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
2. Pronto soccorso	.01	Gestione organizzativa P.S.	Verbale di Pronto Soccorso (Registri, schede triage, schede di pazienti accolti in PS e trasferiti in altro ospedale. Schede di pazienti entrati in PS che rifiutano il ricovero)	ILLIMITATO	
	.02	Attività emergenza - urgenza	Verbale di Pronto Soccorso (Referti)	ILLIMITATO	
	.02	Attività emergenza - urgenza	Documentazione O.B.I. (Osservazione Breve Intensiva)	ILLIMITATO	
	.02	Attività emergenza - urgenza	Documentazione 118 compilata dalle équipe di soccorso dei MSB (Mezzi di Soccorso di Base, con soccorritori a bordo), dei MSI (Mezzi di Soccorso Intermedio, con infermiere a bordo) e dei MSA (Mezzi di Soccorso Avanzato, con medico e infermiere a bordo)	ILLIMITATO Conservazione da parte della Struttura ospedaliera di destinazione del paziente (in cartella clinica o quale parte integrante della documentazione di Pronto Soccorso)	
	.02	Attività emergenza - urgenza	Registrazioni audio della consulenza specialistica telefonica dei Centri Antiveleno	ILLIMITATO	Trattasi di documentazione nativa digitale che deve essere obbligatoriamente trasferita al conservatore dell'ente sulla base di quanto prescritto dal D.Lgs. 82/05 s.i.m.
	.02	Attività emergenza - urgenza	Documentazione sanitaria sia in formato cartaceo sia digitale relativa alla consulenza specialistica telefonica effettuata dai Centri Antiveleno	ILLIMITATO	
	.02	Attività emergenza - urgenza	Documentazione dei Centri Antiveleno	5 anni	Risoluzione CEE 90/C 329/03
3. Assistenza ospedaliera	.01	Aspetti generali, organizzativi e gestionali	Registri nosologici / rubriche ricoverati	ILLIMITATO	Circ. Min. Sanità n. 61 del 19/12/1986
	.02	Ricovero (ordinario, day hospital, day surgery)	Cartella clinica di ricovero comprensiva di tutti i documenti costitutivi, es.: richiesta di ricovero / rapporto di pronto soccorso, consensi, scheda di dimissione ospedaliera (SDO), scheda infermieristica / ostetrica, lettera di dimissione, atti di nascita, referti indagini strumentali e di laboratorio, documenti inerenti la valutazione del dolore ai sensi della legge 38 del 2010, TSO, consulenze specialistiche, ecc.	ILLIMITATO	Circ. Min. Sanità n. 61 del 19/12/1986
	.02	Ricovero (ordinario, day hospital, day surgery)	Verbale - registro operatorio	ILLIMITATO	Circ. Min. Sanità n. 61 del 19/12/1986, Circ. Min. Sanità n. 900 del 14/03/96
	.02	Ricovero (ordinario, day hospital, day surgery)	Cartella clinica di ricovero diurno. Comprensiva di tutti i documenti costitutivi.	ILLIMITATO	Circ. Min. Sanità n. 61 del 19/12/1986 e DPR n. 1409 del 30/06/63 "Legge archivistica"
	.03	Day service	Documentazione inerente le attività ambulatoriali di Day Service	30 anni solo per il Day service chirurgico; 10 anni dalla chiusura del fascicolo per gli altri, assimilabili a documentazione ambulatoriale	
	.04	Assistenza al parto	Registro dei parti e Registro degli aborti	ILLIMITATO	Vedi anche II.3.05
	.04	Assistenza al parto	Certificato di Assistenza al Parto (CedAP)	ILLIMITATO se in cartella clinica; altrimenti 30 anni	
	.04	Assistenza al parto	PMA - Fecondazione eterologa: record relativi a ciascun donatore (screening e i risultati dei test)	30 anni dall'utilizzo	
	.05	Assistenza domiciliare	Cartella clinica di ospedalizzazione domiciliare	ILLIMITATO	DGR 7180 del 24 aprile 2008
	.06	Medicina penitenziaria	Cartella clinica di pazienti in regime detentivo	ILLIMITATO	
	.07	Assistenza psichiatrica e neuropsichiatrica infantile	Cartella clinica di struttura semiresidenziale, Centro Diurno e Residenzialità Leggera. Documentazione relativa alla neuropsichiatria dell'infanzia e dell'adolescenza.	10 anni	
	.07	Assistenza psichiatrica e neuropsichiatrica infantile	Cartella clinica di struttura residenziale (diario clinico, visite psichiatriche, attività riabilitative, colloqui psicoterapeutici, ecc.). Documentazione relativa alla neuropsichiatria dell'infanzia e dell'adolescenza.	ILLIMITATO	
	.07	Assistenza psichiatrica e neuropsichiatrica infantile	Documentazione del sistema informatizzato regionale PSICHE	Secondo tipologia di regime di erogazione della prestazione (residenziale / semiresidenziale)	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 3 - Area Ospedaliera

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Assistenza ambulatoriale	.01	Prestazioni ambulatoriali	Referto di singole prestazioni ambulatoriali. Fascicolo / <i>cartella</i> ambulatoriale con relativa documentazione a supporto	10 anni dalla chiusura del fascicolo per documentazione ambulatoriale. 30 anni solo per attività chirurgica.	
	.01	Prestazioni ambulatoriali	Prescrizione – proposta - ricetta per richieste di prestazioni sanitarie	ILLIMITATO se in cartella clinica; 5 anni altri esemplari	Nota Regione Lombardia H1.2003.0001436. Allegato 3 alla DGRV11I8I78 del 18.02.2002
	.01	Prestazioni ambulatoriali	Referti / documentazione a supporto dell'attività ambulatoriale - percorso chirurgico (Chirurgia a bassa complessità assistenziale)	30 anni	
	.01	Prestazioni ambulatoriali	Referti esami di laboratorio	5 anni	Nota Regione Lombardia H1.2003.0001436. Allegato 3 alla DGRV11I8I78 del 18.02.2002
	.01	Prestazioni ambulatoriali	Schede di emodialisi	10 anni da cessazione di trattamento	
	.01	Prestazioni ambulatoriali	Elenco emodializzati	10 anni da ultima dialisi	
	.01	Prestazioni ambulatoriali	Registro regionale di dialisi	10 anni da ultima dialisi	
	.01	Prestazioni ambulatoriali	Referti radiologici e di medicina nucleare. Compresi i referti strutturati	ILLIMITATO (in caso di ricovero da includere in cartella clinica)	D.M. Sanità 14/02/1997 Intesa Stato - Regioni del 04/04/2012 sul documento del Ministero della Salute recante "Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini – Normativa e prassi"
	.01	Prestazioni ambulatoriali	Documentazione iconografica radiologica e di medicina nucleare. Compresa qualsiasi immagine diagnostica, indipendentemente dalle modalità di acquisizione (analogica o digitale) e dal regime di erogazione (ambulatoriale o ricovero)	10 anni	D.M. Sanità 14/02/1997 Circ. Min. Sanità n. 61 del 19/12/1986 Intesa Stato - Regioni del 04/04/2012 sul documento del Ministero della Salute recante "Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini – Normativa e prassi"
	.01	Prestazioni ambulatoriali	Cartelle radioterapiche	ILLIMITATO	
	.01	Prestazioni ambulatoriali	Certificati di idoneità e inidoneità sportiva	5 anni	D.M. Sanità 18/02/1982 ("Norme per la tutela sanitaria dell'attività sportiva agonistica")

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 3 - Area Ospedaliera

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Assistenza ambulatoriale	.01	Prestazioni ambulatoriali	Referti esami citologici e istologici	10 anni	
	.01	Prestazioni ambulatoriali	Riserva non campionata (residui di campioni biotipici / operatori / autotipici in liquido fissativo)	15 giorni dalla definizione della diagnosi (valido anche per campioni eseguiti durante ricovero)	Si fa riferimento a campioni per esclusive attività diagnostiche. Lo smaltimento può essere anche solo parziale nell'ipotesi di dover prelevare nuovamente o rivedere a distanza una parte del campione; in questo caso va registrato cosa non viene smaltito. LG "Tracciabilità, raccolta, trasporto, conservazione e archiviazione di cellule e tessuti per indagini diagnostiche di anatomia patologica" Consiglio Superiore di Sanità - Sez. I del maggio 2015
	.01	Prestazioni ambulatoriali	Inclusioni in paraffina di campioni istologici derivati da qualsiasi fonte (es. prelievo biotipico, operatorio, autotipico, ecc.)	50 anni (valido anche per campioni eseguiti durante ricovero)	
	.01	Prestazioni ambulatoriali	Campioni istologici allestiti (anche da citoinclusi)	50 anni (valido anche per campioni eseguiti durante ricovero) 15 giorni per i preparati colorati con immunofluorescenza (in quanto soggetti a decadimento. Validi anche per campioni eseguiti durante ricovero)	Per "campione istologico" o "sezione istologica" si fa riferimento sia a quella derivata da Surgical Pathology sia da procedura autotipica. Il fine della lunga conservazione dei campioni è la garanzia per il paziente e i suoi familiari di poter accedere nel tempo, per scopi sanitari, a una fonte di DNA.
	.01	Prestazioni ambulatoriali	Campioni istologici digitalizzati	30 anni (dall'eliminazione del campione istologico "fisico") corrispondente. Validi anche per campioni eseguiti durante ricovero)	Il "vetrino digitale" può essere eseguito ed eliminato dopo il suo utilizzo innumerevoli volte sino a quando è presente il suo corrispettivo "fisico". Nel caso quest'ultimo venga eliminato allo scadere del suo tempo minimo di conservazione appare buona prassi effettuare una sua "scannerizzazione finale" da conservare per il tempo minimo definito. La digitalizzazione appare di particolare rilievo per i preparati in immunofluorescenza che decadono molto rapidamente nel tempo.
	.01	Prestazioni ambulatoriali	Campioni citologici allestiti (escluso Pap test)	50 anni se campione patologico unico, altrimenti 5 anni (valido anche per campioni eseguiti durante ricovero)	Il fine della lunga conservazione dei campioni è la garanzia per il paziente e i suoi familiari di poter accedere nel tempo, per scopi sanitari, a una fonte di DNA e, quando positivo, per confrontare nel tempo l'istotipo e il grado di differenziazione della neoplasia. Nel caso il campione citologico positivo sia associato a un campione istologico o nell'archivio di una Anatomia Patologica sia presente almeno un campione istologico o autotipico dello stesso paziente, i campioni citologici possono essere smaltiti dopo 5 anni.
	.01	Prestazioni ambulatoriali	Pap test	10 anni (valido anche per campioni eseguiti durante ricovero)	
	.01	Prestazioni ambulatoriali	Campioni citologici digitalizzati	30 anni (dall'eliminazione del campione citologico corrispondente. Validi anche per campioni eseguiti durante ricovero)	Il "vetrino digitale" può essere eseguito ed eliminato dopo il suo utilizzo innumerevoli volte sino a quando è presente il suo corrispettivo "fisico". Nel caso quest'ultimo venga eliminato allo scadere del suo tempo minimo di conservazione appare buona prassi effettuare una sua "scannerizzazione finale" da conservare per il tempo minimo definito.
	.01	Prestazioni ambulatoriali	Residui di campioni citologici in fase liquida	3 mesi dall'emissione del referto diagnostico (valido anche per campioni eseguiti durante ricovero)	I campioni citologici in fase liquida possono essere utilizzati per indagini immunocitochimiche o biomolecolari, senza necessità di riprelevare il paziente. Il tempo minimo indicato di archiviazione considera i tempi che potrebbero intercorrere tra la diagnosi, il ricevimento di questa da parte del clinico e la sua richiesta di approfondimenti diagnostici.
	.01	Prestazioni ambulatoriali	Residui di acidi nucleici estratti da campioni istologici o autotipici o da liquidi biologici risultati idonei alle indagini di patologia molecolare già effettuate.	2 anni (valido anche per campioni eseguiti durante ricovero)	

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 3 - Area Ospedaliera

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
5. Riabilitazione	.01	Riabilitazione	Cartella ambulatoriale di riabilitazione	10 anni da ultima registrazione	
6. Attività Immuno-trasfusionale	.01	Aspetti generali, organizzativi e gestionali	Documentazione inerente il sistema qualità e le relative registrazioni del sangue ed emocomponenti	10 anni	D.M. 2 novembre 2015 "Disposizioni relative ai requisiti di qualità e sicurezza del sangue e degli emocomponenti". Art. 29, comma 4.
	.02	Valutazione idoneità donatori sangue ed emocomponenti	Cartella sanitaria del donatore di sangue ed emocomponenti	30 anni	D.M. 2 novembre 2015 "Disposizioni relative ai requisiti di qualità e sicurezza del sangue e degli emocomponenti". Art. 5, comma 8.
	.02	Valutazione idoneità donatori sangue ed emocomponenti	Le registrazioni dei risultati riguardanti le determinazioni del gruppo sanguigno ABO ed Rh, della presenza di anticorpi irregolari anti-eritrocitari, delle prove di compatibilità pre-trasfusionali relativi ai pazienti riceventi, nonché la documentazione inerente le reazioni ed eventi avversi gravi.	15 anni	D.M. 2 novembre 2015 "Disposizioni relative ai requisiti di qualità e sicurezza del sangue e degli emocomponenti". Art. 29, comma 3.
	.02	Valutazione idoneità donatori sangue ed emocomponenti	Documentazione che consente di ricostruire il percorso di ogni unità di sangue ed emocomponenti, il modulo di consenso informato relativo a ciascuna donazione, i risultati delle indagini di validazione prescritte dalla normativa vigente su ogni unità di sangue o emocomponenti	30 anni	D.M. 2 novembre 2015 "Disposizioni relative ai requisiti di qualità e sicurezza del sangue e degli emocomponenti". Art. 29, comma 2.
	.02	Valutazione idoneità donatori sangue ed emocomponenti	Danni da trasfusione	ILLIMITATO	L. 210/1992 art.3 e L. 238/1997; Circ. 1 Ministero della Sanità del 4-11-1996 n. 900
7. Attività di trapianto d'organi e tessuti	.01	Aspetti generali, organizzativi e gestionali	Documentazione gestionale (Segnalazione alla Direzione Sanitaria di soggetto in morte cerebrale, Attivazione della commissione per l'accertamento dello stato di morte cerebrale, Verbale di accertamento della morte cerebrale, Richiesta di nulla osta dell'autorità giudiziaria)	30 anni	D.Lgs. n.16/2010. - 30 anni per i dati inerenti il donatore e il ricevente (art. 14 c. 2) - 10 anni per le registrazioni dell'istituto dei tessuti (all. V lett. E)
	.02	Donazione e prelievo	Dati necessari ad assicurare la tracciabilità in tutte le fasi per la donazione, l'approvvigionamento, il controllo, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani.	30 anni dopo l'uso clinico (l'archiviazione dei dati può avvenire anche in forma elettronica)	D.Lgs. 6 novembre 2007, n. 191 "Attuazione della direttiva 2004/23/CE sulla definizione delle norme di qualità e di sicurezza per la donazione, l'approvvigionamento, il controllo, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani"
	.02	Donazione e prelievo	Dati per identificare donatore, donazione, tessuti / cellule, ecc. (di cui all'allegato X del D.Lgs. 25 gennaio 2010, n. 16)	30 anni	D.Lgs. 25 gennaio 2010, n. 16 "Attuazione delle direttive 2006/17/CE e 2006/86/CE, che attuano la direttiva 2004/23/CE per quanto riguarda le prescrizioni tecniche per la donazione, l'approvvigionamento e il controllo di tessuti e cellule umani, nonché per quanto riguarda le prescrizioni in tema di rintracciabilità, la notifica di reazioni ed eventi avversi gravi e determinate prescrizioni tecniche per la codifica, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani". (Art. 14, comma 2).
	.02	Donazione e prelievo	I registri dei donatori, necessari ai fini di una completa tracciabilità,	30 anni dopo l'uso clinico o dopo la scadenza o eliminazione del tessuto o cellula in un archivio adeguato	D.Lgs. 25 gennaio 2010, n. 16 "Attuazione delle direttive 2006/17/CE e 2006/86/CE, che attuano la direttiva 2004/23/CE per quanto riguarda le prescrizioni tecniche per la donazione, l'approvvigionamento e il controllo di tessuti e cellule umani, nonché per quanto riguarda le prescrizioni in tema di rintracciabilità, la notifica di reazioni ed eventi avversi gravi e determinate prescrizioni tecniche per la codifica, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani". (Allegato IV, Punto 1.4.4)
	.02	Donazione e prelievo	Tutte le registrazioni, dati grezzi compresi, critiche per la sicurezza e la qualità dei tessuti e cellule.	10 anni dopo la data di scadenza, l'uso clinico o lo smaltimento	D.Lgs. 25 gennaio 2010, n. 16 "Attuazione delle direttive 2006/17/CE e 2006/86/CE, che attuano la direttiva 2004/23/CE per quanto riguarda le prescrizioni tecniche per la donazione, l'approvvigionamento e il controllo di tessuti e cellule umani, nonché per quanto riguarda le prescrizioni in tema di rintracciabilità, la notifica di reazioni ed eventi avversi gravi e determinate prescrizioni tecniche per la codifica, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani". (Allegato V, E, punto 7)
	.02	Donazione e prelievo	Tracciabilità del percorso di idoneità, assegnazione degli organi, prelievo e trapianto organi.	30 anni dopo la donazione	D.M. del 19 novembre 2015 "Attuazione della direttiva 2010/53/UE relativa alla norme di qualità e sicurezza degli organi umani destinati ai trapianti"

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 3 - Area Ospedaliera

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
8. Farmaceutica ospedaliera	.01	Farmaceutica	Matrici ricette del SSN (a cura dei singoli medici dal 1/09/2005 e comunque per i ricettari "nominali")	5 anni dalla data dell'ultima prescrizione	Nota DG Sanità Regione Lombardia H1.2001.0033136 del 16/05/2001 Nota DG Sanità Regione Lombardia H1.2005.0032866 del 04/07/2005 Allegato (p. 3.3) al Decreto Ministeriale 18 maggio 2004
	.01	Farmaceutica	Documentazione relativa all'approvvigionamento farmaci	5 anni	
	.01	Farmaceutica	Documenti di trasporto per consegna beni farmaceutici	10 anni	
	.01	Farmaceutica	Documentazione inerente alla gestione dei controlli di qualità sui gas medicinali	10 anni	
	.01	Farmaceutica	Schede di prescrizione dei farmaci in file F	2 anni	Comunicazione DG Sanità prot. H12004.0057563 del 11.11.2004
	.01	Farmaceutica	Documentazione piani terapeutici farmaci	ILLIMITATO (in cartella clinica)	
	.01	Farmaceutica	Fogli di lavorazione delle preparazioni di farmaci oncologici	5 anni	Raccomandazione ministeriale sulla sicurezza dei farmaci antitumorali
	.01	Farmaceutica	Grafici di rilevazione della temperatura registrazione linea del freddo (frigoriferi per medicinali)	1 anno	
	.02	Stupefacenti	Registri di entrata e uscita degli stupefacenti	10 anni dalla data dell'ultima registrazione per enti e imprese autorizzati alla fabbricazione 5 anni dalla data dell'ultima registrazione per le officine autorizzate all'impiego e per le imprese autorizzate al commercio all'ingrosso 2 anni dalla data dell'ultima registrazione per le farmacie aperte al pubblico e le farmacie ospedaliere	DPR n.390/90 art. 60 e s.i.m. comma 1 Nota Regione Lombardia H1.2014.0019108 del 27.05.2014 Legge n. 38 del 15.03.2010 art. 10
	.02	Stupefacenti	Buoni / ordini di acquisto stupefacenti e documenti trasporto / fatture	10 anni	
	.02	Stupefacenti	Bollettario con moduli approvvigionamento (Reparti - Farmacia) di farmaci stupefacenti	2 anni dalla data dell'ultima registrazione	Decreto del Presidente della Repubblica del 9 ottobre 1990, n. 309 - art. 45, comma 6. Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza.
	.02	Stupefacenti	Bollettario con moduli restituzione (Reparti - Farmacia) di farmaci stupefacenti	5 anni dalla data dell'ultima registrazione	Decreto del Presidente della Repubblica del 9 ottobre 1990, n. 309 - art. 45, comma 6. Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza.
	.02	Stupefacenti	Registro di carico e scarico dei medicinali contenenti sostanze stupefacenti o psicotrope delle Unità Operative (reparti) delle Aziende Sanitarie	2 anni dalla data dell'ultima registrazione	Decreto Ministeriale 3 agosto 2001 in riferimento a Decreto del Presidente della Repubblica del 9 ottobre 1990, n. 309 - art. 60 c. 3 e 6. Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza.

MASSIMARIO DEL SISTEMA SOCIO SANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIO SANITARIO DI REGIONE LOMBARDIA rev04
TITOLO 3 - Area Ospedaliera

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
9. Medicina legale ospedaliera	.01	Medicina necroscopica	Certificato di morte, accertamento morte, cause di morte (ISTAT), referti autoptici	ILLIMITATO	
	.01	Medicina necroscopica	Registro dei decessi	ILLIMITATO	
	.02	Indennizzo danni	Giudizio medico-legale per danni da vaccinazioni e/o trasfusioni	ILLIMITATO	Circ. Min. Sanità 10 aprile 1992
	.03	Consulenze medico-legali	Certificazioni medico-legali; certificati inerenti accertamenti di laboratorio a valenza medico-legale; attività peritale; giudizio medico-legale per danni da vaccinazioni e/o trasfusioni	10 anni	In considerazione del termine di prescrizione del diritto al risarcimento del danno subito da un paziente che è di dieci anni, siffatta documentazione verrà conservata sino al compimento della prescrizione decennale.
10. Medicina del lavoro	.01	Cartella sanitaria e di rischio del lavoratore	Cartelle sanitarie e di rischio	Almeno sino alla cessazione del rapporto di lavoro; 40 anni dalla cessazione del lavoro comportante una esposizione ad agenti cancerogeni ; 30 anni dalla cessazione del lavoro comportante una esposizione a radiazioni ionizzanti	D.M. 12/07/07, n.155
	.01	Cartella sanitaria e di rischio del lavoratore	Schede delle prove allergologiche relative a malattie professionali	ILLIMITATO	Normativa di riferimento difforme, per lo più a carattere regionale.
	.02	Malattia professionale e infortunio sul lavoro	Registri vaccinazioni	ILLIMITATO	
	.02	Malattia professionale e infortunio sul lavoro	Registri infortuni	4 anni dall'ultima registrazione e, se non usato, dalla data in cui è stato vidimato	D.M. 12/9/58, art.2
11. Sperimentazione clinica dei medicinali e dei dispositivi	.00	Sperimentazione clinica dei medicinali e dei dispositivi	Documentazione relativa alla sperimentazione clinica <i>dei</i> farmaci e dei dispositivi (fascicolo della sperimentazione) <i>per uso umano</i>	25 anni dalla conclusione della sperimentazione	L'art. 58, comma 1 del regolamento EU 536/14 sulla sperimentazione dei medicinali sull'uomo, dispone quanto segue: "A meno che il diritto dell'Unione preveda un periodo di archiviazione maggiore, il promotore e lo sperimentatore conservano il contenuto del fascicolo permanente della sperimentazione clinica per almeno venticinque anni dalla conclusione della medesima. Tuttavia, le cartelle cliniche dei soggetti sono archiviate in conformità del diritto nazionale".
	.00	Sperimentazione clinica dei medicinali e dei dispositivi	Consenso informato relativo all'esposizione a radiazioni ionizzanti a scopo di ricerca scientifica e clinica e area sperimentazione di farmaci	ILLIMITATO	D.Lgs. n.230/1995 e D.M. 18/03/1998

PIANO DI CONOSCENZA PER LA SICUREZZA DI ARCHIVI E BIBLIOTECHE

PREMESSA

Il tema dell'emergenza è stato ampiamente trattato negli ultimi anni, molti sono stati gli studi pubblicati e anche le linee guida (tra tutte, quella della Direzione Generale degli Archivi del giugno 2014¹) o normative emanate in proposito². Questo lavoro nasce proseguendo nella direzione tracciata da quanto precedentemente concluso, cercando di aggiungere considerazioni e indicazioni più pratiche che possano contribuire a costruire una mentalità di prevenzione, inserendo il Piano di Reazione all'Emergenza in una visione più ampia, sistemica, in cui questa è solo la fase di un processo circolare che passa necessariamente dalla conservazione e manutenzione continua, per ridurre significativamente il livello di rischio residuo.

Il presente lavoro si propone di trattare il tema della conservazione dei beni contenuti in archivi o biblioteche, prevedendo delle misure di protezione per ridurre quanto più possibile gli impatti derivanti da rischi di varia natura e dimensione, con particolare attenzione agli eventi accidentali³, che obbligano ad azioni di carattere eccezionale per la salvaguardia dei beni tutelati e conservati.

L'approccio proposto, in quanto volto soprattutto alla conservazione del patrimonio librario ed archivistico, risulta applicabile (quasi) indistintamente per entrambe le realtà; per questo motivo, i beni "librari" e "archivistici" vengono sostituiti nel presente testo dal termine più generico "bene" e "archivio"⁴ e biblioteca vengono quindi considerati allo stesso modo nell'affrontare questo argomento.

¹ http://www.archivi.beniculturali.it/images/pdf_articoli/servizio%20il%20gruppi%20di%20lavoro/emergenze/Linee%20guida%20emergenze.pdf

² Particolare riferimento sono in questo senso le direttive e circolari del MiBACT in materia di gestione delle emergenze, quali: MiBAC, Circolare n. 132 8 ottobre 2004, *Piani di emergenza per la tutela del patrimonio culturale*, MiBAC, Circolare n.30 6 febbraio 2007, *Piani di emergenza per la tutela del patrimonio culturale – pianificazione e gestione delle esercitazioni*, MiBACT, Direttiva 12 dicembre 2013, *Procedure per la gestione delle attività di messa in sicurezza e salvaguardia del patrimonio culturale in caso di emergenze derivanti da calamità naturali*, MiBACT, Direttiva 23 aprile 2015, *Aggiornamento della direttiva 12 dicembre 2013, relativa alle Procedure per la gestione delle attività di messa in sicurezza e salvaguardia del patrimonio culturale in caso di emergenze derivanti da calamità naturali*.<

³ È necessario precisare che le cause esaminate in questo piano sono essenzialmente di tipo accidentale, come sopra accennato. Questo però non esclude tutta una serie di danni, che chiameremo "quiescenti" che seppur non derivanti da eventi improvvisi hanno nelle conseguenze lo stesso tipo di effetto, ossia l'uscita momentanea dalla disponibilità del bene, se non la perdita definitiva. Il danno "quiescente" è dovuto allo scarso o mancato monitoraggio dei depositi o parti di essi dove le condizioni microclimatiche e la manutenzione siano assenti. Nel caso del danno quiescente l'emergenza si evidenzia quando si rileva casualmente un danno riguardante un numero (spesso rilevante) di beni conservati nel medesimo locale. I beni subiscono ed evidenziano un danno conforme alle conseguenze di un allagamento: viene rilevato un diffuso sviluppo di muffe, compattamento, indebolimento degli adesivi e dei collanti, ecc... in questo caso pur non essendo un evento emergenziale ab origine lo si deve trattare in modo simile per le conseguenze che i beni hanno subito. Bisogna considerare quindi il danno per "quiescenza" un danno subdolo del quale non il fato crudele (un tubo che si rompe ad esempio) è il responsabile ma la condizione e la gestione "ordinaria" dei depositi.

⁴ Solo per evidenziare differenze logiche fra due realtà matericamente simili ma per contenuto diverse, si intende precisare quanto

Il bene è l'oggetto che questo piano si prefigge di tutelare nella sua integrità materica, di qualsiasi natura e forma esso sia e a qualsivoglia forma di gestione, conservazione e fruizione sia soggetto; scopo ultimo è quello di ridurre e gestire al meglio i rischi presenti, prevedendo, in caso di calamità, le forme di intervento immediato e di recupero più adatte ad ogni specifica condizione. E' necessario qui precisare che un bene, dal momento che perde le caratteristiche per essere fruito perde la sua funzione primaria di essere disponibile alla consultazione e studio e quindi depaupera l'istituto che lo tutela o lo possiede, che perde almeno parte dello scopo per cui lavora ed ha una sua legittimità.

È comunque fondamentale sottolineare che, data la pluralità di materiali che è possibile ritrovare in un archivio, sarà necessario considerare che alcuni di questi debbano prevedere una risposta al danneggiamento che sia specifica per le loro caratteristiche intrinseche e dovranno quindi ricevere trattamenti immediati, tempestivi ed effettuati da personale specializzato⁵.

Il Piano di Conoscenza per la Sicurezza intende rappresentare uno strumento di gestione dell'archivio o della biblioteca in cui poter analizzare e ricomporre tutte le indicazioni sulla sicurezza e lo stato del bene, provenienti da studi pregressi e piani sovraordinati⁶, a cui è possibile affiancare ulteriori e specifiche valutazioni, nell'ottica di garantire un incremento del livello di protezione del bene. La stessa raccolta dei dati può evidenziare anche delle imprecisioni operative che possono essere corrette immediatamente. Integrando perciò le fasi di analisi e valutazione dei rischi nel complessivo processo di gestione dell'archivio/biblioteca, si estende la validità e l'importanza della cultura di protezione e salvaguardia oltre la fase della sola emergenza e dell'intervento post evento catastrofico, contribuendo a garantire una reale ed efficace conservazione preventiva e programmata, mettendo in atto tutte quelle azioni che hanno come fine la prevenzione degli eventi che potrebbero danneggiare i

segue.

Nello specifico, con "archivio" si fa riferimento a tre distinti elementi:

- «il complesso dei documenti prodotti o comunque acquisiti da un ente (magistrature, organi e uffici centrali e periferici dello Stato; enti pubblici territoriali e non territoriali; istituzioni private, famiglie e persone, imprese) durante lo svolgimento della propria attività. I documenti che compongono l'Archivio sono pertanto collegati tra loro da un nesso logico e necessario, detto vincolo archivistico.
- Il locale in cui un ente conserva il proprio archivio.
- L'istituto nel quale vengono concentrati archivi di varia provenienza che ha per fine istituzionale la conservazione permanente dei documenti destinati alla pubblica consultazione».

(fonte: <http://www.archivi.beniculturali.it/index.php/abc-degli-archivi/glossario>)

Analogo significato multiplo ha anche il termine *biblioteca*.

⁵ Per maggiori dettagli, si faccia riferimento alle schede specifiche del PRE.

⁶ Si intendono qui tutti i piani di livello più alto (relativi principalmente alle discipline della pianificazione – locale, sovralocale, regionale, nazionale... e della gestione del rischio – riferita alla salute dei lavoratori, di emergenza comunale o infra comunale,...) e che contengono indicazioni utili come base per le analisi da effettuare e delle prescrizioni da dover considerare.

beni, o comunque la diminuzione dei loro effetti negativi.

Il responsabile della tutela e della conservazione dell'Archivio/Biblioteca ha la piena responsabilità di garantire la disponibilità materiale e la fruizione dei beni ivi conservati, raccogliendo tutte le informazioni necessarie, direttamente o tramite le segnalazioni degli altri membri del personale e dell'utenza.

Il piano deve avere un responsabile o un suo referente riconosciuto al quale fare arrivare tutte le informazioni utili al fine che ci si propone.

Tutto il personale, in ogni sua mansione e livello condivide la corresponsabilità della conservazione e del monitoraggio, ed è supporto importante per il referente principale.

L'importanza delle pratiche di prevenzione è dimostrata sia dall'efficacia nella riduzione dei rischi che dalla diminuzione del numero di beni perduti a causa dell'impatto di un evento, nonché dei costi derivanti dal sostenere le azioni di recupero e la conseguente inaccessibilità dei beni coinvolti. Pertanto la disponibilità d'uso dei beni è lo scopo che ci si prefigge e che deve essere il principio da tenere presente durante la compilazione delle pratiche di prevenzione e di risposta all'emergenza.

Le operazioni preliminari di conoscenza e la compilazione del PRE sono un valido aiuto in fase di stipula di copertura assicurativa in quanto permettono il contenimento delle perdite, il contenimento dei costi di salvataggio e recupero e quindi una valida ricaduta in fase contrattuale con le compagnie assicurative. In questo caso anche l'aggiornamento del piano assume un'importanza particolarmente rilevante.

Scopo primario del Piano è stimolare una conoscenza più approfondita dell'archivio/biblioteca e favorire una raccolta organizzata delle informazioni pertinenti al fine di:

- ricostruire un quadro preciso sulle **condizioni generali** del sistema composto dal "contenitore" archivio o biblioteca e dal "contenuto", ovvero dall'insieme dei beni conservati,
- valutarne il grado di **vulnerabilità** (intesa come «caratteristica specifica di una comunità o un sistema o di un bene che lo rende suscettibile agli impatti dannosi di un pericolo⁷») soprattutto in riferimento alle correlazioni esistenti tra i due,
- rilevarne il livello di **resilienza** globale (intesa come «l'abilità di un sistema, di una comunità o di una società esposta a pericoli di resistere, assorbire, riparare e riprendersi

⁷UN-ISDR, *Terminology on Disaster Risk Reduction*, <https://www.unisdr.org/we/inform/terminology#letter-v>

tempestivamente ed efficientemente dagli effetti di un pericolo, anche attraverso la preservazione e restaurazione delle sue strutture e funzioni basilari⁸»).

Questa valutazione consente di definire il livello di rischio cui i beni sono specificatamente sottoposti, in modo tale da predisporre le necessarie e più indicate misure di prevenzione e protezione e di progettare e organizzare la risposta ad eventuali emergenze. Per questo motivo una parte consistente del Piano è costituita da analisi preliminari che possano costruire una conoscenza critica e coerente del bene e che possano indirizzare alla progettazione delle misure di controllo e riduzione dei rischi più rispondenti e calibrate rispetto alle effettive caratteristiche e necessità riscontrate, valutando sia le possibili fonti di pericolo del contesto e quindi “esterne” (o “esogene”, di origine umana o naturale come terremoto, alluvioni, incendi, atti vandalici/terrorismo, industrie, altre attività che possono essere svolte nello stesso edificio,...), che quelle “interne” (o “endogene” come incendi, attacchi biologici, rottura di tubazioni, blackout, gestione inefficiente/inappropriata, ...).

Al fine di potersi più agevolmente confrontare e relazionare con i Piani per la Sicurezza esistenti che hanno come scopo la tutela del personale lavoratore⁹ e dell’utenza, il presente documento, che ha come fine la protezione dei beni archivistici/librari, si struttura secondo lo stesso impianto, riproponendo le medesime sezioni, ognuna introdotta da una piccola presentazione con indicazioni ed istruzioni:

1. DVR - Documento di Valutazione dei Rischi: attraverso l’analisi dei piani sovraordinati in materia di gestione del rischio e della sicurezza, delle modalità gestionali, nonché dello stato di conservazione del bene e dell’edificio, Il DVR individua tutti i pericoli presenti e ne quantifica il rischio, ossia la probabilità che ciascun pericolo generi dei danni, tenuto conto della loro entità potenziale¹⁰ (il rischio è la «combinazione della probabilità di accadimento di un evento e delle sue conseguenze negative»¹¹).

⁸ UN-ISDR, *Terminology on Disaster Risk Reduction*, <https://www.unisdr.org/we/inform/terminology#letter-r>

⁹ D.lgs. 9 aprile 2008, n. 81 e s.m.i.

¹⁰ Il sistema a matrice di valutazione dei rischi, proposto in questo documento, è lo strumento analitico attualmente più diffuso per generare e quantificare il rischio residuo e stabilire una priorità rispetto al piano di adeguamento delle misure di prevenzione da inserire, progettare ed attivare.

La diffusione e la popolarità di tale strumento si deve principalmente al fatto che la sua applicazione, una volta assimilate le istruzioni e applicato in maniera coerente, è relativamente semplice e genera in automatico, in base al risultato, una quantificazione del rischio residuo e di conseguenza la priorità degli interventi da porre in essere per limitare il rischio.

¹¹ UN-ISDR, *Terminology on Disaster Risk Reduction*, <https://www.unisdr.org/we/inform/terminology#letter-r> Questa definizione segue quella della ISO 73:2009. Da sottolineare che il termine “rischio” ha due connotazioni distinte: nell’uso popolare l’enfasi è generalmente data al concetto di caso, possibilità (“il rischio di un incidente”), mentre nel vocabolario tecnico l’enfasi è

2. **PMP - Piano delle Misure di Prevenzione**, che raccoglie e sistematizza le contromisure precedentemente individuate per limitare il rischio residuo, suddivise per tipologia (strutturali e non strutturali) e scala di intervento (singolo locale e intero complesso).

3. **PRE - Piano di Risposta all’Emergenza - Archivio/Biblioteca** in cui si raccolgono una serie di indicazioni comportamentali da mettere in atto a seguito di un’emergenza. Quanto più queste operazioni verranno programmate e le condizioni dell’archivio/biblioteca saranno dettagliate in anticipo, tanto più sarà possibile eseguirle in maniera efficiente ed efficace nelle situazioni di stress post evento. Si considerano in questo documento i principali rischi cui un archivio potrebbe essere soggetto nel nostro territorio, ovvero alluvione/allagamento, incendio, sisma.

Il Piano di Risposta all’Emergenza si inserisce nello stesso contesto e fa riferimento alle stesse esigenze a cui sono riferite le disposizioni relative al *piano di Disaster Recovery* ed al *piano di continuità operativa* previsti per le Pubbliche Amministrazioni dal Codice dell’Amministrazione Digitale, direttamente riferiti anche agli archivi in formazione,¹².

Tutte le altre informazioni utili agli scopi finali del Piano sono strutturate in ulteriori documenti di corredo:

PIANO DI ANALISI DELLE RISORSE PRESENTI E ATTIVABILI IN CASO DI EMERGENZA, per riportare e quindi analizzare le risorse (umane, di materiali e mezzi ed economiche) attualmente a disposizione della Biblioteca/Archivio e quelle da reperire a fronte dei pericoli e dei rischi valutati.

PIANO DELLA FORMAZIONE, che pianifica le giornate di formazione del personale, la comunicazione dei contenuti del piano e le esercitazioni delle attività emergenziali. È necessario considerare in questo contesto anche le fasi di concertazione con enti preposti alla gestione del rischio, come ad esempio la Protezione Civile.

PIANO DI MONITORAGGIO E REVISIONE, consiste nell’individuare una serie di indicatori misurabili, attraverso cui poter giudicare l’effettiva efficacia delle indicazioni del piano, per poter prevedere, eventualmente, delle revisioni.

PIANO DI RIPRISTINO l’attività di ripristino, posteriore e conseguente alle attività di messa in sicurezza in risposta all’emergenza, rappresenta uno step fondamentale del processo globale di gestione del rischio. Un adeguato ripristino ha una durata variabile e inizia per alcuni materiali anche in fase

generalmente data alle conseguenze, in termini di “perdite potenziali” per particolari cause. È quindi necessario sottolineare quindi come il medesimo termine, contenga in sé una varietà di significati spesso connessi con la sfera emotiva e percettiva e possa anche far riferimento concetti tra loro diversi ed essere quantificato diversamente se analizzato da più persone.

¹² Codice Amministrazione Digitale (d. lgs. 82/2005 e ss mm ii) art. 50 bis c. 3 lettera b): *Linee guida AgID per il disaster recovery delle pubbliche amministrazioni – aggiornamento 2013*

direttamente successiva all'evento disastroso e prevede l'esecuzione di asciugature, puliture, restauri, scarto, duplicazione, pulizia dei beni. In questa prima stesura verranno dettagliate in modo particolare due metodologie per il trattamento del materiale cartaceo danneggiato: il congelamento e la liofilizzazione.

Al fine di rendere rapidamente interpretabili (anche da operatori esterni o che interverranno nella sola fase, concitata, dell'emergenza) le informazioni raccolte su stato dei beni e dell'archivio/biblioteca, nonché alcune delle prescrizioni previste dal Piano, si consiglia di riportare tutti questi dati non tanto in forma descrittiva, quanto in forma grafica. La creazione di mappe tematiche in cui riassumere sinteticamente gli elementi più significativi, consente innanzitutto di minimizzare i tempi di reazione, di organizzare più speditamente ed efficacemente gli interventi di risposta; la "graficizzazione" permette inoltre di creare una sorta di consuntivo facilmente consultabile delle analisi eseguite da accompagnare al piano e da integrare ed aggiornare in parallelo.

Importanza fondamentale in questo senso è rivestita dal rilievo topografico dei beni conservati in archivio/biblioteca, a cui associare le valutazioni relative al livello di urgenza di intervento sui materiali (per maggiori indicazioni su questa operazione, riferirsi a *Analisi dell'Archivio/Biblioteca a livello dei singoli locali - Rappresentazione del locale, inventario topografico e codici di urgenza*)

Il piano non ha, naturalmente, la pretesa di essere esaustivo, né si può pretendere l'eshaustività nella predisposizione dei documenti richiesti. Le linee guida fornite costituiscono dei consigli per organizzare ed eseguire delle azioni logiche che hanno come il fine il contenimento massimo del danno.

Il Piano si propone come un documento flessibile, facilmente integrabile ed aggiornabile, con la possibilità di affiancare i potenziali compilatori tramite l'istituzione di un'attività di tutoraggio preliminare di cui saranno referenti le rispettive Soprintendenze competenti per territorio.

SOMMARIO

PREMESSA.....	2
SOMMARIO.....	8
INFORMAZIONI GENERALI SUL PIANO.....	10
DVR - DOCUMENTO DI VALUTAZIONE DEI RISCHI DELL'ARCHIVIO.....	14
ANALISI DELL'ARCHIVIO/BIBLIOTECA A LIVELLO COMPLESSIVO.....	16
ANALISI E VALUTAZIONE DEI RISCHI a livello complessivo.....	19
ANALISI DELL'ARCHIVIO/BIBLIOTECA a livello dei singoli locali	24
ANALISI E VALUTAZIONE DEI RISCHI a livello dei singoli locali	29
PMP - PIANO DELLE MISURE DI PREVENZIONE	33
PIANO DI ANALISI DELLE RISORSE PRESENTI E ATTIVABILI IN CASO DI EMERGENZA.....	35
PRE - PIANO DI RISPOSTA ALL'EMERGENZA.....	38
INFORMAZIONI PRELIMINARI	38
RISCHIO ALLAGAMENTO	42
RISCHIO INCENDIO	51
RISCHIO TERREMOTO.....	55
PIANO DI RIPRISTINO.....	56
Liofilizzazione - introduzione.....	57
Liofilizzazione di materiale cartaceo (a cura di Davide Fissore e Antonello Barresi, DISAT, Politecnico di Torino, Laboratorio di Liofilizzazione).....	60
PIANO DELLA FORMAZIONE	69
PIANO DI MONITORAGGIO E REVISIONE.....	70
ALLEGATO 1 - SCHEDA RILEVAZIONE DANNI.....	72

SOPRINTENDENZA ARCHIVISTICA e BIBLIOGRAFICA DELLA LOMBARDIA

Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche

A cura di Paola Mussini, Luciano Sassi – giugno 2016

ALLEGATO 2a - SCHEDA PRONTO INTERVENTO	75
ALLEGATO 2b - REPORT INTERVENTO	77
ALLEGATO 3 – ETICHETTA CASSE	78
RIFERIMENTI	79
VALUTAZIONE DEL RISCHIO	79
PROCEDURE E INTERVENTI.....	80
LIOFILIZZAZIONE.....	81

INFORMAZIONI GENERALI SUL PIANO

Redatto da

Informazioni e contatti del bene o dei soggetti che hanno partecipato alla redazione dei piani, specificandone i ruoli e le competenze.

In data

Segnalare la data di compilazione.

Validità

L'aggiornamento dei dati contenuti nel presente piano va eseguito con cadenza annuale e comunque in occasione di ogni evento di rilievo (del personale responsabile, spostamenti di materiale archivistico, attività di inventariazione, modifiche nel sistema gestionale, eventi dannosi, interventi strutturali all'edificio,...), in modo tale da verificarne e confermarne la fattibilità e validità.

Revisioni

Revisore	Motivazione	Data

In base a quanto sopra specificato, riportare nella tabella i principali dati di riferimento per le revisioni del documento e segnalare la successiva.

Luoghi in cui si conserva copia del piano

È importante condividere i contenuti del Piano con tutti i soggetti coinvolti e renderlo altresì accessibile sempre, anche in assenza del responsabile.

Specificare se si tratta di copia digitale/cartacea, se presente nell'archivio stesso, in uffici dell'ente gestore, presso protezione civile, vigili del fuoco,...

Elenco dei soggetti coinvolti

Elencare gli enti ed i singoli soggetti coinvolti nella gestione e conservazione degli archivi presenti, nonché nella produzione e messa in pratica delle indicazioni del Piano.

- ...

SOPRINTENDENZA ARCHIVISTICA e BIBLIOGRAFICA DELLA LOMBARDIA*Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche**A cura di Paola Mussini, Luciano Sassi – giugno 2016*

•		
Contatti		
Si riportano di seguito i contatti principali dei soggetti coinvolti nelle operazioni di gestione dell'emergenza, derivati dall'analisi delle risorse condotta alla sezione PIANO DI ANALISI DELLE RISORSE PRESENTI E ATTIVABILI IN CASO DI EMERGENZA divisi per "contatti interni" ovvero del personale dell'archivio/biblioteca in questione, di enti esterni che si occupano di gestire e garantire dei servizi alla struttura e i contatti degli organi istituzionali di protezione e vigilanza da allertare in caso di emergenza.		
Contatti interni		
RESPONSABILE EMERGENZA Nome:	ufficio:	
	casa:	
	cellulare:	
SOSTITUTO Nome:	ufficio:	
	casa:	
	cellulare:	
DIRETTORE Nome:	ufficio:	
	casa:	
	cellulare:	
SQUADRA INTERVENTO	Nome:	cellulare:
		ufficio:
		casa:
	Nome:	cellulare:
		ufficio:
		casa:
Nome:	cellulare:	
	ufficio:	
	casa:	

SOPRINTENDENZA ARCHIVISTICA e BIBLIOGRAFICA DELLA LOMBARDIA*Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche**A cura di Paola Mussini, Luciano Sassi – giugno 2016*

ADDETTO ALLE RELAZIONI ESTERNE Nome:	ufficio:
	casa:
	cellulare:

<i>Contatti esterni</i> Indicare il numero di assistenza in emergenza oppure quello del referente specifico.	
GESTORE RETE ELETTRICA	
GESTORE RETE GAS	
IMPRESE MANUTENZIONE IMPIANTI	
ENTE GESTORE DELLA SICUREZZA DEI LAVORATORI	
RESTAURATORE	
IMPRESE SPECIALIZZATE PER L'EMERGENZA	
IMPRESE DI TRASPORTO/AUTOMEZZI	
MAGAZZINI REFRIGERATI	
IMPRESE OUTSOURCING	
FORNITURE ANTI INFORTUNISTICA	

<i>Contatti organi di protezione e vigilanza</i>	
VIGILI DEL FUOCO	115
EMERGENZA SANITARIA	118
POLIZIA	113

SOPRINTENDENZA ARCHIVISTICA e BIBLIOGRAFICA DELLA LOMBARDIA*Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche**A cura di Paola Mussini, Luciano Sassi – giugno 2016*

CARABINIERI	112
VIGILI DEL FUOCO	115
CARABINIERI TUTELA PATRIMONIO ARTISTICO <i>Legione "Lombardia", via Della Moscova 19 2021 Milano</i>	0262765122
PROTEZIONE CIVILE	800 061 160

DVR - DOCUMENTO DI VALUTAZIONE DEI RISCHI DELL'ARCHIVIO

Questa sezione del Piano prevede una ricognizione sistematica dello stato di fatto del bene analizzato e dei beni archivistici e librari ivi conservati.

Si richiede di analizzare le condizioni esistenti, al fine di comprendere quali siano i pericoli principali cui i beni archivistici/librari possano essere soggetti, al fine di meglio programmare e predisporre le contromisure più efficaci per limitare l'entità dei danni causate da un possibile evento disastroso.

Il bene archivio/biblioteca viene indagato e rilevato a **due livelli** di approfondimento e di scala.

Livello complessivo: l'archivio/biblioteca viene considerato nel complesso della sede che lo ospita, nell'insieme di tutti i beni che lo compongono, di tutti i locali che lo ospitano, delle varie interrelazioni esistenti; le valutazioni di priorità verranno in questo caso effettuate a scala più ampia; livello di singolo locale: è necessario effettuare valutazioni specifiche circa lo stato di conservazione dei beni conservati e degli ambienti, nonché l'attribuzione di un codice che identifichi la priorità richiesta per l'intervento sullo specifico bene, nonché sull'importanza di garantire continuità operativa all'ente in caso di emergenza.

Nel caso di entità molto complesse, potrebbe essere utile aumentare i livelli di approfondimento del piano, considerando anche, ad esempio, la sede, l'edificio ed il piano di riferimento.

Ne consegue che anche l'identificazione dei pericoli e delle vulnerabilità, la valutazione dei rischi, la proposta delle contromisure necessarie per la loro riduzione, la descrizione delle risorse disponibili, verranno eseguite a tutti i livelli. Questa distinzione mira anche a guidare più agevolmente l'individuazione dei fattori di rischio insistenti a livello esogeno (esterni) ed endogeno (interni).

Seguendo lo stesso principio di scalabilità, anche il Piano stesso può essere integrato da analisi e valutazioni ulteriori e di maggior dettaglio, considerate in questa sede accessorie e non obbligatorie, presentabili sotto forma di allegato¹³.

Il sistema di valutazione analitico proposto, si basa sulla compilazione della matrice dei rischi, seguendo il principio basato sulla relazione

$$R = P \times I, \text{ dove:}$$

il rischio (R) è dato dal valore di Probabilità (P) di accadimento di un dato evento, moltiplicato per la stima dei danni e impatti (I) conseguenti; R è espresso in una scala di valori da 1 a 6, corrispondenti ai

¹³ Un ulteriore possibile approfondimento potrebbe sottolineare l'interazione tra loro dei pericoli individuati, nel tentativo di comprendere le catene di eventi che potrebbero verificarsi.

giudizi *molto basso, basso medio, alto, molto alto, estremo*. Ovviamente questa categorizzazione può, in accordo alle esigenze specifiche, essere semplificata riducendo, ad esempio le categorie di impatto e/o di probabilità.

Questo metodo risulta di facile applicabilità e consente di legare immediatamente il danno atteso ad ogni pericolo alle contromisure necessarie da mettere in atto (nella tabella successiva alla matrice di calcolo del rischio)¹⁴.

¹⁴ La metodologia di calcolo e valutazione proposta può ovviamente essere maggiormente raffinata, anche con l'aiuto di discipline più specifiche e specialistiche di supporto alle decisioni, come l'analisi multicriteria AHP- Analytic Hierarchy Process e la Fuzzy Logic.

ANALISI DELL'ARCHIVIO/BIBLIOTECA A LIVELLO COMPLESSIVO
<i>Denominazione¹⁵</i>
Riportare la denominazione univoca dell'edificio i cui si conservano i beni da tutelare.
<i>Indirizzo</i>
Localizzazione dell'edificio, indicazione, se possibile, anche delle coordinate geografiche con indicazione del sistema di riferimento.
<i>Destinazioni d'uso presenti</i>
Segnalare le destinazioni d'uso presenti nell'edificio: questa informazione può essere utile nel valutare possibili interferenze, nella definizione dei pericoli e nella progettazione delle attività emergenziali*. *Queste informazioni sono facilmente reperibili dagli eventuali Piani di Prevenzione ed Emergenza per i lavoratori.
<i>Localizzazione dell'edificio nell'area urbana</i>
Descrittiva (centro storico, periferia, extra-urbano) e cartografica. Questo dato aiuta a individuare la presenza di particolarità geomorfologiche del sito che possono risultare quali fattori di vulnerabilità intrinseca o pericoli esterni. È importante verificare inoltre la connessione strutturale con gli edifici circostanti (soprattutto in zona sismica).
<i>Archivi presenti</i>
<i>Segnalare quali archivi sono conservati e per facilità di individuazione e disambiguazione, segnarne la collocazione su una planimetria.</i>
<i>Metri lineari complessivi di documentazione</i>
<i>Note significative</i>
Riportare qui tutte le informazioni che si ritengono significative agli scopi della gestione dei rischi presenti e della risposta all'emergenza (livello di inventariazione, presenza di topografico,..)
<i>Localizzazione dell'archivio/biblioteca all'interno dell'edificio</i>
Descrittiva e planimetrica: segnalare il numero di piani dell'edificio, il numero di piani occupati dall'archivio e i locali con una segnalazione di massima dei contenuti. E' possibile che l'archivio sia

¹⁵ Per l'individuazione delle informazioni da raccogliere si è fatto anche riferimento alle schede SIUSA Complesso Archivistico, dalle quali – se presenti – possono essere ricavate

conservato in edifici distinti, in questo caso è necessario segnalarli tutti.

La/le planimetria/e dovranno fornire un quadro di tutte le componenti e dei collegamenti verticali, specificandone anche il materiale costruttivo e la percorribilità in caso di emergenza.

È importante in questa sede riportare inoltre: vie di fuga, uscite di sicurezza, terminali impianti di sicurezza (antincendio, antintrusione)*.

*Queste informazioni sono facilmente reperibili dagli eventuali Piani di Prevenzione ed Emergenza per i lavoratori.

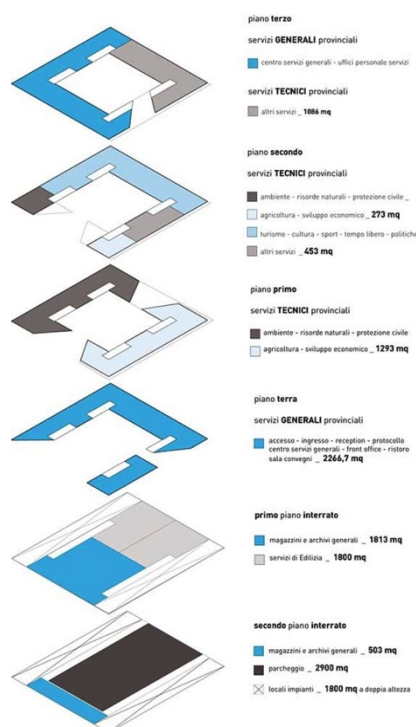


Figura 1. Esempio di planimetrie dei vari piani dell'edificio in cui segnare destinazioni d'uso, collocazioni, collegamenti verticali ed orizzontali e tutti gli elementi salienti ai fini della valutazione dei rischi.

Numero di piani occupati

Numero e indicazione dei piani occupati dai singoli archivi presenti.

Numero di locali

Numero di locali in cui si conservano gli archivi presenti, definire un codice univoco di identificazione di ciascuno.

Stato di conservazione dell'edificio

La segnalazione di criticità rilevanti a livello di strutture, paramenti, funzioni, arredi, impianti...è utile a definire un livello complessivo dello stato dell'edificio soprattutto in riferimento ai beni conservati*.

*Valutazione riferita a specifiche relazioni tecniche, ove esistenti.

<i>Rilievo fotografico</i> Riportare riferimenti precisi agli elementi e alle situazioni descritte, con immagini georeferite (segnare su una mappa i punti di presa). Una descrizione di questo tipo consente una ricostruzione accurata del bene in precisi momenti e facilita l'analisi dell'evoluzione di alcuni fenomeni nel tempo e l'attribuzione delle rispettive responsabilità.
<i>Segnalazione di eventuali interventi pregressi/in corso</i> Produrre una lista degli interventi a quali l'archivio/biblioteca è stato sottoposto (sia come contenitore che come contenuto), motivarne l'esecuzione (a seguito di danni, impatti, eventi calamitosi, adeguamenti funzionali/strutturali) e indicare se il materiale documentario ha subito danni, se è stato spostato, se sono occorsi cambiamenti gestionali. Questa sorta di consuntivo tecnico e scientifico permette di ricostruire agevolmente la storia dell'edificio nonché dell'archivio/biblioteca, facilitando il riconoscimento e l'analisi di determinate problematiche, che potrebbero rendere più vulnerabile la documentazione in caso di calamità.
<i>Impianti</i> Mappatura , descrizione e rilievo fotografico degli impianti, delle centraline e dei terminali presenti. Segnalare possibili criticità, danni o malfunzionamenti. Questi contenuti possono essere desunti da altri piani/progetti riguardanti l'archivio/biblioteca. • Elettrico • Idraulico • Monitoraggio ambientale • Climatizzazione • Antincendio • Antintrusione • Movimentazione • ... Eseguire delle prove di chiusura/spegnimento periodiche per verificarne il funzionamento, riportare nella tabella iniziale (INFORMAZIONI GENERALI SUL PIANO) tutti i dati relativi ai vari fornitori di energia.
<i>Vie di fuga</i> Segnalare i percorsi possibili per lo spostamento del materiale archivistico in caso di emergenza. Le informazioni a riguardo reperibili dagli eventuali Piani di Prevenzione ed Emergenza (DVR e Piano di

Emergenza) per i lavoratori dovranno essere adeguate e/o integrate a seconda delle specifiche necessità e caratteristiche dei beni conservati e dei luoghi.

Accessi

Segnalare gli accessi presenti, indicando anche le eventuali caratteristiche specifiche dei serramenti (porte REI, antiallagamento, antieffrazione,...).

Le informazioni a riguardo reperibili dagli eventuali Piani di Prevenzione ed Emergenza per i lavoratori dovranno essere adeguate e/o integrate a seconda delle specifiche necessità e caratteristiche dei beni conservati e dei luoghi.

Accessibilità

Segnalare se l'archivio è accessibile e da chi, considerando motivo, durata, limitazioni.

Indicare, se presenti, barriere architettoniche.

Attribuzione di codici di urgenza ai singoli locali

Questa operazione è fondamentale ai fini della programmazione della risposta all'eventuale emergenza, in quanto consente di localizzare, a questo livello a scala macro, quali siano i locali nei quali sarà più urgente intervenire in caso di emergenza. Si consiglia pertanto, per facilità di strutturazione, di eseguire questa valutazione a conclusione della redazione del topografico di dettaglio (a livello di singolo fondo e/o documento), come descritta nella scheda per l'analisi dell'archivio/biblioteca.

Lo scopo è quello di ottenere, a seguito risultante della valutazione della priorità di intervento attribuita ad ogni singolo fondo o bene contenuto nell'archivio/biblioteca in questione, una planimetria dell'edificio in cui segnalare i locali in cui è preferibile intervenire prioritariamente in caso di evento calamitoso, in quanto contenenti i beni ritenuti in questo senso privilegiati (per valore, stato di conservazione, ...).

ANALISI E VALUTAZIONE DEI RISCHI a livello complessivo

Connessione con piani di Emergenza e di Analisi del rischio sovraordinati

Verifica delle prescrizioni imposte, con riferimento alle analisi contenute nei piani sovraordinati (ovvero i piani che a livelli territoriali più ampi – di edificio, comunale, provinciale, regionale – si occupano di analisi e gestione dei rischi esistenti, come indicato nell'elenco sottostante) mediati rispetto alla serie storica degli avvenimenti quando possibile (questo significa che sarebbe necessario valutare l'effettivo grado di rischio presente anche rispetto al numero degli eventi recentemente verificatosi; ad esempio il Piano di Assetto Idrogeologico considera scenari di inondazione riferibili a tempi di ritorno spesso molto lunghi e non coerenti con l'effettiva frequenza di accadimento).

ANALISI DI RISCHIO		PIANIFICAZIONE TERRITORIALE
Piano di Emergenza dell'edificio		PTR – Piano Territoriale Regionale
Certificato Prevenzione Incendi		PTCP – Piano Territoriale di Coordinamento Provinciale
Documento di Valutazione dei Rischi		PGT – Piano di Gestione del Territorio
Piano di Emergenza Comunale		...
PAI, Piano Alluvioni		
RIR		
Piano AIB		
Microzonazione sismica		
...		
<i>Identificazione dei pericoli (rif. Documento di Valutazione dei Rischi e Piano di Emergenza)</i>		
Classificati in ordine di possibilità di accadimento (segnalazione della fonte). Si specificano di seguito tipologie riferite ad un evento specifico nel tempo e non ad azioni prolungate (incuria/abbandono, cambiamento climatico), i cui impatti vanno comunque considerati, se presenti, come moltiplicatore della vulnerabilità intrinseca del bene.		
DI ORIGINE AMBIENTALE	DI ORIGINE ANTROPICA	TECNOLOGICI
Incendio	Atti vandalici/terrorismo	Blackout
Alluvione	Industriale	Malfunzionamento/rottura impianti
Allagamento	Na-Tech (ovvero eventi tecnologici innescati da eventi naturali)	Malfunzionamento/rottura terminali
Terremoto		ICT (tecnologie Informatiche)
Frana	...	...
Attacco biologico		
<i>Contromisure esistenti</i>		
Sistemi di allertamento, spegnimento, antintrusione, monitoraggio,...		
Queste barriere impediscono il verificarsi di alcuni eventi o il propagarsi del danno, tutto ciò che queste non riescono a “bloccare” va a costituire il “rischio residuo”, ovvero quello che può presentarsi in emergenza.		
<i>Vulnerabilità</i>		
La vulnerabilità è definita come la propensione a subire un danneggiamento a seguito dell'impatto di un pericolo di determinato tipo e intensità.		
Data la difficile quantificazione di questo dato, si richiede un'analisi solamente qualitativa.		

Elencare qui i fattori e le condizioni che possono aumentare le conseguenze generate da ogni possibile evento/pericolo, ad esempio:

- mancanza/assenza di manutenzione e/o ispezione periodica dello stato di conservazione,
- assenza di dispositivi di monitoraggio ambientale,
- assenza di dispositivi di spegnimento incendi,
- assenza di personale specializzato nell'intervento in emergenza,
- assenza di procedure per l'emergenza,
- assenza di materiali e mezzi,
- impropri metodi di archiviazione,
- uso di strutture inadatte,
- presenza di degradi strutturali/superficiali nei locali,
- vulnerabilità intrinseche dei beni correlate ai materiali, contenuti, valore,
- ...

Matrice per il calcolo del rischio (metodo semi-quantitativo)

La matrice va compilata per ogni rischio presente, è necessario definire a priori la corrispondenza numerica di ogni giudizio che può essere accompagnato da una descrizione qualitativa¹⁶.

E' possibile prevedere dei fattori correttivi che rispecchino lo stato di conservazione o la presenza di eventuali vulnerabilità precedentemente individuate.

Scopo di questa operazione è principalmente portare il compilatore (conservatore e gestore del bene) a ragionare sulla possibile incidenza di eventuali fenomeni e alla correlazione tra le possibili conseguenze e la probabilità di accadimento. Un' analisi di questo tipo, calata nella realtà specifica e filtrata dalle conoscenze dell'operatore, porta all'individuazione degli elementi che devono ricevere maggiore attenzione nell'immediato.

	IMPATTI				
	IRRILEVANTE	BASSO	RILEVANTE	MOLTO RILEVANTE	SEVERO
	1	2	3	4	5

¹⁶ Per approfondimento, si consiglia l'utilizzo di tecniche di supporto alle decisioni multicriterio [AHP - Analytic Hierarchy Process (Brokerhof et al., 2007)] e di Fuzzy logic (Shang & Hossan, 2013) per stabilire i pesi specifici e la gravità dei danni, traducendo il giudizio "linguistico" in fattore numerico e stabilire criteri di valutazione.

SOPRINTENDENZA ARCHIVISTICA e BIBLIOGRAFICA DELLA LOMBARDIA

Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche

A cura di Paola Mussini, Luciano Sassi – giugno 2016

PROBABILITÀ	QUASI SICURO 5	Medio	Alto	Molto alto	Estremo	Estremo
	PROBABILE 4	Medio	Medio	Alto	Molto alto	Estremo
	MODERATA 3	Basso	Medio	Medio	Alto	Molto alto
	IMPROBABILE 2	Molto basso	Basso	Medio	Medio	Alto
	RARO 1	Molto basso	Molto basso	Basso	Medio	Medio

LIVELLO DI RISCHIO	AZIONE DA INTRAPRENDERE	SCALA TEMPORALE entro cui intervenire
Molto basso	Monitoraggio delle condizioni rilevate	/
Basso	Instaurare un sistema di verifica che consenta di mantenere nel tempo le condizioni di sicurezza preventivate	Appena possibile
Medio	Programmare analisi più dettagliate della fonte di pericolo e delle eventuali incidenze sugli elementi più vulnerabili per meglio definire le contromisure da adottare	6 mesi – 1 anno
Alto	Predisporre gli strumenti necessari a minimizzare il rischio ed a verificare la efficacia delle azioni preventivate	6 mesi
Molto alto	Intervenire al più presto sulla fonte di rischio, provvedendo ad eliminare le anomalie che portano alla determinazione di livelli di rischio non accettabili	1-2 mesi
Estremo	Intervenire immediatamente sulla fonte di rischio, provvedendo a sospendere le lavorazioni sino al raggiungimento di livelli di rischio accettabili	Immediatamente

Interpretazione dei risultati

Descrizione del processo di valutazione eseguito e dei risultati ottenuti, alla luce dello stato attuale del bene. Considerazioni di massima soprattutto per le situazioni di pericolo a rischio alto/molto alto/estremo.

Valutazione dei possibili impatti (metodo qualitativo)

In aggiunta al metodo semi-quantitativo, è possibile effettuare una valutazione qualitativa per scenari (costruzione di scenari evidenziando la possibile concatenazione di effetti secondari).

In questo contesto si ritiene questa analisi ulteriore e non strettamente indispensabile.

ANALISI DELL'ARCHIVIO/BIBLIOTECA a livello dei singoli locali ¹⁷
<i>Codice identificativo del locale</i>
Riportare il codice del locale cui si fa riferimento, come indicato nelle planimetrie alla scheda e condurre le successive analisi per ciascun locale dell'archivio/biblioteca in cui siano conservati documenti.
<i>Descrizione e rappresentazione</i>
Descrizione generale del locale, planimetria e prospetti interni. Segnalazione delle misure salienti, collocazione degli scaffali e loro distanza da pareti e altro mobilio.
<i>Superficie</i>
Indicare la superficie in metri quadri del locale.
<i>Altezza</i>
Se possibile, indicare l'altezza massima e minima del locale.
<i>Aperture interne</i>
Indicare il numero, la disposizione e l'eventuale collegamento con altri locali. Indicare tipologia e stato di conservazione dei serramenti.
<i>Aperture esterne</i>
Indicare il numero, la disposizione, tipologia e stato di conservazione dei serramenti.
<i>Passaggi</i>
Indicare, se presenti, zone di passaggio di rilevata criticità (fisica, funzionale, gestionale,...). È importante individuare un passaggio che sia sufficientemente ampio per svolgere in sicurezza le operazioni di movimentazione (che consenta il passaggio con i carrelli, ad esempio e che sia privo di ostacoli).
<i>Arredi</i>
Segnalare la presenza di arredi mobili o fissi, il loro materiale (alcuni possono essere più o meno indicati in presenza di pericoli specifici) e la loro posizione (potrebbe interferire con le azioni di recupero).
<i>Pavimentazione</i>

^{17 17} Per l'individuazione delle informazioni da raccogliere si è fatto anche riferimento alle schede SIUSA (descrittivo e gestionale), dalle quali – se presenti – possono essere ricavate

SOPRINTENDENZA ARCHIVISTICA e BIBLIOGRAFICA DELLA LOMBARDIA*Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche**A cura di Paola Mussini, Luciano Sassi – giugno 2016*

Indicare la tipologia di pavimentazione presente, nonché possibili degradi presenti.
Valutare attentamente la possibile “sciovolosità” di alcuni materiali, soprattutto in presenza di acqua (o anche ghiaccio), per prevenire adeguatamente possibili danni agli operatori: a questo proposito è necessario dotarsi di materiale per rivestirli e apporre strisce antiscivolo soprattutto sulle scale a cui si è obbligati a far ricorso durante la risposta all’emergenza,....
<i>Personale presente</i>
Stima del personale che mediamente è presente nel locale in un dato orario.
<i>Uso*</i>
Indicare se il locale sia ad uso esclusivo o promiscuo
<i>Metri lineari scaffalature esistenti*</i>
<i>Caratteristiche salienti*</i>
Segnalare in questa sede: • quanto spazio sugli scaffali sia rimasto libero per consentire eventuali incrementi, • la consistenza dell’archivio con una descrizione schematica riportante i dati fondamentali delle unità di archivio, • il numero complessivo di unità conservate, • i metri lineari totali
<i>Materiale</i>
Indicare i principali materiali di cui sono composti gli elementi presenti in ogni locale (carta, pergamena, cuoio, etc).
<i>Ordinamento presente*</i>
Sì/No
<i>URL descrizione analitico*</i>
<i>Estremi cronologici*</i>
Estremo remoto
Estremo recente
<i>Rilievo fotografico del luogo</i>

Possibilmente con localizzazione dei punti di presa sulla mappa e con riferimenti incrociati di elementi precedentemente descritti.	
<i>Stato del locale*</i>	
Descrizione dello stato di conservazione del locale e presenza di elementi salienti (impianti, degradi superficiali, etc...).	
Impianto elettrico	
Misure antincendio	
Misure antintrusione	
Impianto di climatizzazione	
Impianto di movimentazione	
Altro	
<i>Scaffalature</i>	
Descrizione e rilievo fotografico delle tipologie utilizzate (armadi, rastrelliere, compactus e dei materiali (metallo, legno, ...) Evidenziare sistemi di ancoraggio (a terra, tra scaffali, al soffitto, alle pareti,...). I documenti sono sollevati da terra? Di quanti cm? Sì/No	
<i>Rappresentazione del locale, inventario topografico e codici di urgenza</i>	
Questa operazione è fondamentale ai fini della programmazione della risposta all'eventuale emergenza, in quanto consente di disporre di una mappa precisa dei beni conservati, distinti per il livello urgenza di intervento. A questo proposito è necessario redigere preliminarmente un inventario topografico anche schematico, che localizzi precisamente i fondi/le collezioni all'interno dell'edificio; a questo punto è necessario valutare ogni elemento in base ad una serie di parametri costruiti secondo le proprie specificità ed ai quali ogni istituto fa riferimento , ma che dovrebbero sicuramente considerare ad esempio l'unicità, l'alto valore culturale o amministrativo, , ecc... La mappatura delle urgenze deve definire: denominazione tradizionale, segnatura, localizzazione esatta, quantità, sviluppo in metri lineari, misure caratterizzanti (altezza minima, massima e prevalente necessarie per evidenziare difficoltà di trasporto/spostamento in caso di evacuazione rapida e quindi di	

particolari necessità di reperimento materiali e mezzi per la movimentazione), supporti (carta, pergamena, altro, misti).

Il livello di priorità può essere segnalato con un simbolo associato ad un colore¹⁸ da apporre sulle scaffalature.

La mappa, destinata ad essere aggiornata periodicamente, o almeno quando intervengano modifiche di rilievo per uno o più dei parametri esaminati, offre lo schema fondamentale per procedere alla successiva fase di pianificazione.

È importante sottolineare come l'ordine di priorità di cui si tratta in questo contesto non abbia un valore assoluto, ma risponda a un principio pragmatico; è infatti finalizzato alla selezione di quantità ragionevoli di materiali da salvare nelle diverse fasi di intervento, consentendo così agli addetti di razionalizzare gli sforzi e le risorse disponibili rispetto al tempo disponibile per l'efficacia dell'intervento.

Attribuire un valore relativo è un'attività essenziale, anche se comporta una serie di scelte non sempre facili e gradevoli. Privilegiare o sacrificare, anche se ancora sulla carta, alcune collezioni rispetto alle altre è una decisione difficile, ma è sicuramente di maggiore efficacia operativa rispetto al comportamento opposto, con il quale, evitando qualunque scelta a priori, si rischia di dover salvare disordinatamente quello che capita, affidandosi al puro caso.

Nella letteratura professionale sull'argomento sono individuati numerosi criteri utili per la determinazione del valore di un fondo, di una collezione, o di un singolo volume o documento, particolarmente utile in questo senso risulta la classificazione messa a punto da Bertini (2005).

L'obiettivo finale della valutazione è quello di ricondurre le diverse porzioni del patrimonio sottoposto a valutazione a tre categorie fondamentali:

Alta priorità (corrispondente ai materiali sui quali devono concentrarsi gli sforzi dei soccorritori nelle prime 8 ore successive al sinistro);

Media priorità (i materiali sui quali intervenire nelle successive 24 ore):

Bassa priorità (i materiali che possono essere anche sacrificati, se il tempo e le risorse a disposizione non consentono il loro recupero).

E' consigliabile che a ciascuna di queste categorie sia fatto corrispondere un codice colore (es. rosso =

¹⁸ L'accorgimento di accoppiare colore e forma potrebbe risultare particolarmente utile anche per facilitare operatori con difficoltà visive (daltonici, ad esempio). Una possibile combinazione potrebbe essere: triangolo rosso per i beni di elevata importanza, quadrato giallo o arancione per quelli di seconda urgenza, cerchio verde per i restanti.

alta priorità; giallo = media priorità; verde = bassa priorità) da utilizzare in apposita segnaletica a scaffale, oppure in speciali mappe a disposizione dei soccorritori, conservate in luogo sicuro e facilmente raggiungibile in caso di emergenza.

A queste tre categorie può aggiungersi un gruppo ristrettissimo di pezzi unici (i ‘magnifici dieci’) che qualificano il patrimonio della biblioteca o dell’archivio. Questi cimeli, conservati in condizioni di sicurezza, devono poter essere reperiti e portati in salvo rapidamente, anche da una sola persona. È naturalmente cruciale che le informazioni relative alla localizzazione di questi cimeli rimangano riservate, ma che, in caso di emergenza, siano accessibili anche in assenza del direttore dell’istituto attraverso una procedura codificata.

In ogni caso è utile ricordare che si dovrà dare la precedenza ai documenti che sono essenziali perché l’ente possa continuare a svolgere il proprio mandato ovvero quelli per la protezione dei diritti legali e finanziari; i piani di emergenza e le direttive connesse, i documenti di sistema per le informazioni in formato digitale, i documenti atti a proteggere i diritti del personale nonché quelli relativi ai pagamenti e alle pensioni. Sicuramente vanno messi in salvo gli inventari archivistici e gli schedari di biblioteca dei quali sarebbe utile averne una copia in altro luogo sicuro (backup del catalogo, inventario).

E’ sicuramente utile produrre delle schede descrittive e grafiche riportanti piante e prospetti principali (rappresentazione “scatolare” anche con l’ausilio di foto-raddrizzamenti) in cui evidenziare la collocazione degli scaffali e di tutti gli elementi e le misure/distanze salienti.

ANALISI E VALUTAZIONE DEI RISCHI a livello dei singoli locali

Identificazione dei pericoli (rif. Documento di Valutazione dei Rischi e Piano di Emergenza)

Rispetto all'analisi condotta precedentemente a livello globale (ANALISI E VALUTAZIONE DEI RISCHI) sarà necessario soffermarsi sui pericoli specifici che possano essere rilevanti a livello di singolo locale, quindi, probabilmente si tratterà di considerare maggiormente gli elementi presenti all'interno dell'edificio.

DI ORIGINE AMBIENTALE	DI ORIGINE ANTROPICA	TECNOLOGICI
Incendio	Atti vandalici/terrorismo	Blackout
Alluvione	Industriale	Malfunzionamento/rottura impianti
Allagamento	Na-Tech (ovvero eventi tecnologici innescati da eventi naturali)	Malfunzionamento/rottura terminali
Terremoto		ICT (Tecnologie Informatiche)
Frana	...	...
Attacco biologico		

Contromisure esistenti

Sistemi "fisici" di allertamento, spegnimento, antintrusione, monitoraggio, nonché gestionali, come la presenza di procedure . Queste barriere impediscono il verificarsi di alcuni eventi o riducono gli impatti o la loro propagazione, tutto ciò che queste non riescono a "bloccare" va a costituire il "rischio residuo", ovvero quello che può presentarsi in emergenza.

Vulnerabilità

Propensione del bene a subire un danneggiamento a seguito dell'impatto di un pericolo di determinato tipo e intensità. Data la difficile quantificazione di questo dato, si richiede un'analisi solamente qualitativa.

Elencare qui i fattori e le condizioni che possono aumentare le conseguenze generate da ogni possibile evento/pericolo, ad esempio:

- mancanza/assenza di manutenzione e/o ispezione periodica dello stato di conservazione dei beni,
- assenza di dispositivi di monitoraggio ambientale,
- assenza di dispositivi di spegnimento incendi,
- assenza di personale specializzato nell'intervento in emergenza,

- assenza di procedure per l'emergenza,
- assenza di materiali e mezzi,
- impropri metodi di archiviazione,
- uso di strutture inadatte,
- presenza di degradi strutturali/superficiali nei locali,
- vulnerabilità intrinseche dei beni correlate ai materiali, contenuti, valore,
- ...

Matrice per il calcolo del rischio (metodo semi-quantitativo)

La matrice va compilata per ogni rischio presente, è necessario definire a priori la corrispondenza numerica di ogni giudizio che può essere accompagnato da una descrizione qualitativa¹⁹.

E' possibile prevedere dei fattori correttivi che rispecchino lo stato di conservazione o la presenza di eventuali vulnerabilità precedentemente individuate.

Scopo di questa operazione è principalmente portare il compilatore (conservatore e gestore del bene) a ragionare sulla possibile incidenza di eventuali fenomeni e alla correlazione tra le possibili conseguenze e la probabilità di accadimento. Un' analisi di questo tipo, calata nella realtà specifica e filtrata dalle conoscenze dell'operatore, porta all'individuazione degli elementi che devono ricevere maggiore attenzione nell'immediato.

		IMPATTI				
		IRRILEVANTE	BASSO	RILEVANTE	MOLTO RILEVANTE	SEVERO
		1	2	3	4	5
PROBABILITÀ	QUASI SICURO 5	Medio	Alto	Molto alto	Estremo	Estremo
	PROBABILE 4	Medio	Medio	Alto	Molto alto	Estremo
	MODERATA 3	Basso	Medio	Medio	Alto	Molto alto
	IMPROBABILE 2	Molto basso	Basso	Medio	Medio	Alto

¹⁹ Per approfondimento, si consiglia l'utilizzo di tecniche di supporto alle decisioni multicriterio [AHP - Analytic Hierarchy Process (Brokerhof et al., 2007)] e di Fuzzy logic (Shang & Hossan, 2013) per stabilire i pesi specifici e la gravità dei danni, traducendo il giudizio "linguistico" in fattore numerico e stabilire

SOPRINTENDENZA ARCHIVISTICA e BIBLIOGRAFICA DELLA LOMBARDIA

Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche

A cura di Paola Mussini, Luciano Sassi – giugno 2016

	RARO 1	Molto basso	Molto basso	Basso	Medio	Medio

LIVELLO DI RISCHIO	AZIONE DA INTRAPRENDERE	SCALA TEMPORALE entro cui intervenire
Molto basso	Monitoraggio delle condizioni rilevate	/
Basso	Instaurare un sistema di verifica che consenta di mantenere nel tempo le condizioni di sicurezza preventivate	Appena possibile
Medio	Programmare analisi più dettagliate della fonte di pericolo e delle eventuali incidenze sugli elementi più vulnerabili per meglio definire le contromisure da adottare	6 mesi – 1 anno
Alto	Predisporre gli strumenti necessari a minimizzare il rischio ed a verificare la efficacia delle azioni preventivate	6 mesi
Molto alto	Intervenire al più presto sulla fonte di rischio, provvedendo ad eliminare le anomalie che portano alla determinazione di livelli di rischio non accettabili	1-2 mesi
Estremo	Intervenire immediatamente sulla fonte di rischio, provvedendo a sospendere le lavorazioni sino al raggiungimento di livelli di rischio accettabili	Immediatamente

Interpretazione dei risultati

Descrizione del processo di valutazione eseguito e dei risultati ottenuti, alla luce dello stato attuale del bene. Considerazioni di massima soprattutto per le situazioni di pericolo a rischio alto/molto alto/estremo.

Valutazione dei possibili impatti (metodo qualitativo)

In aggiunta al metodo semi-quantitativo, è possibile effettuare una valutazione qualitativa per scenari (costruzione di scenari evidenziando la possibile concatenazione di effetti secondari).

In questo contesto si ritiene questa analisi ulteriore e non strettamente indispensabile.

PMP - PIANO DELLE MISURE DI PREVENZIONE

In questa sezione si porta il compilatore del Piano a definire, in base alle analisi dello stato di fatto effettuate per la Valutazione dei Rischi precedentemente condotta, quali contromisure siano più efficaci per limitare quanto più possibile la probabilità del verificarsi di un rischio oppure i danni conseguenti.

Le misure di protezione possono così essere procedure operative per rendere più efficiente la gestione dell'archivio/biblioteca in un'ottica di prevenzione e protezione (definite qui "**misure non strutturali**"), oppure degli adeguamenti fisici ("**strutturali**") per contenere e limitare i danni, prevenirne il verificarsi tramite, ad esempio, il monitoraggio, l'ispezione e la manutenzione continuativa o la dotazione di specifiche attrezzature.

Nella scelta finale delle contromisure adottabili, è bene considerare anche il criterio di sostenibilità inteso come minimo intervento, ma anche economica come giusta proporzione tra costi e benefici e la scala di applicazione (per singolo locale e per intero complesso).

È necessario in questa sede essere il più concreti possibili e quindi programmare nel tempo l'introduzione delle misure di prevenzione previste, a partire da quella valutata come più urgente per la protezione e salvaguardia dei beni dell'Archivio/Biblioteca.

Contromisure strutturali necessarie

Le valutazioni derivanti dalla compilazione delle sezioni precedenti del presente documento, potrebbero evidenziare la necessità di prevedere la realizzazione di alcune contromisure per la riduzione di un rischio specifico (che diminuiscano la vulnerabilità o il livello di esposizione, che aumentino il grado di resilienza del sistema, ...).

Alcune contromisure strutturali potrebbero essere:

- dotazione di sistema di allertamento,
- dotazione di sistema di monitoraggio,
- dotazione di sistema di spegnimento automatico,
- rinforzo strutturale di porzioni di edificio,
- sostituzione di scaffalature/dotazioni non adeguate,
- restauro,
- catalogazione e inventariazione,
- programmazione di rilievi ed analisi specifiche,
- ...

SOPRINTENDENZA ARCHIVISTICA e BIBLIOGRAFICA DELLA LOMBARDIA

Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche

A cura di Paola Mussini, Luciano Sassi – giugno 2016

PERICOLO	LIVELLO DI RISCHIO	CONTROMISURE	PROGRAMMAZIONE

Contromisure non strutturali (gestionali) necessarie

Alcune tipologie di danno possono essere prevenute con l'applicazione di misure per intervenire sulle modalità di gestione del bene. Sicuramente un piano e la pratica costante della manutenzione programmata e preventiva possono diminuire notevolmente i livelli di rischio presenti.

PERICOLO	LIVELLO DI RISCHIO	CONTROMISURE	PROGRAMMAZIONE

Alcune contromisure gestionali da tenere in considerazione:

- redazione e verifica Piano di manutenzione programmata,
- redazione di codici di pratica e comportamento per gli operatori coinvolti a vari livelli,
- manutenzione e verifica del funzionamento dei vari impianti, nonché degli allacciamenti alla rete esterna,
- formazione del personale interno e volontario,
- esecuzione del monitoraggio fisico e strumentale (soprattutto utile per la valutazione di pericoli "quiescenti" cfr. **Premessa**). Stabilire quale sia il range ottimale - tendendo ad un valore ottimale di U.R. fra il 45% ed il 65% considerando che più è alta l'umidità relativa con l'innalzamento della temperatura si ottiene un più veloce sviluppo di muffe. I valori dei parametri ambientali idonei da regolare e mantenere in riferimento alle caratteristiche specifiche dei beni e in risposta alle istanze di conservazione, accessibilità e consultazione, sono parte del normale processo di conservazione e debbono essere quelli a cui si deve ritornare in fase di ripristino ambientale,
- concertazione con enti coinvolti nelle azioni di salvataggio (Protezione Civile, Vigili del Fuoco,...),
- ...

PIANO DI ANALISI DELLE RISORSE PRESENTI E ATTIVABILI IN CASO DI EMERGENZA

Una volta analizzata nel dettaglio la condizione attuale del bene archivio/biblioteca, individuati i pericoli che ne minacciano la conservazione, valutato il livello di rischio conseguente e verificate le più efficaci contromisure da adottare, è necessario comprendere di quali risorse (capitale finanziario e umano, materiali e mezzi) sia necessario disporre per fronteggiare l'eventuale emergenza.

Si richiede pertanto una ricognizione delle risorse disponibili e un elenco ragionato di quelle da reperire anticipatamente.

La risposta all'emergenza è direttamente proporzionale all'entità dell'evento, alla disponibilità di personale ed agli spazi necessari per il recupero dei beni danneggiati.

Sono i beni danneggiati o in pericolo il solo obiettivo dell'azione che ci si prefigge, attivandosi inoltre per ottenere il rientro del bene nel minor tempo possibile nelle disponibilità dell'ente proprietario o tutelante.

L'obiettivo in fase di emergenza è bloccare il progredire degli effetti dell'impatto causato dall'evento, solo successivamente nei tempi e modi necessari, ci si impegnerà a recuperare e a ripristinare il bene per renderlo nuovamente disponibile alla consultazione; i tempi di recupero sono proporzionali ai danni subiti ed alle risorse impiegate.

Personale struttura operativa

Personale presente, qualifica e attività prevalente, affidamento di compiti relativi alla gestione delle emergenze. Si occuperanno della fase di salvataggio dei beni coloro che rivestono ruoli per la sicurezza del personale lavoratore.

Materiali e mezzi

Elenco dei materiali e mezzi eventualmente a disposizione o da reperire, utili per la gestione dell'emergenza.

Un elenco più specifico dei materiali utili per fronteggiare i diversi tipi di rischio sono riportati nella sezione PRE - PIANO DI RISPOSTA ALL'EMERGENZA

Dispositivi per la movimentazione interna del materiale

Descrizione e localizzazione di carrelli e dispositivi per la movimentazione del materiale all'interno dell'edificio.

<i>Aree disponibili</i>
E' fondamentale individuare con anticipo le zone più sicure e più facilmente accessibili in cui eseguire gli interventi di primo intervento.
<i>Aree interne per il ricovero temporaneo</i>
Individuare possibili aree sicure dell'edificio in cui poter stoccare temporaneamente il materiale danneggiato od in pericolo di esserlo.
<i>Modalità di trasporto</i>
Programmare le modalità di trasporto del materiale danneggiato nei depositi, eventualmente predisporre delle convenzioni specifiche con vettori: è importante verificare la rispondenza dei loro mezzi e metodi ai requisiti di conservazione e sicurezza dei beni.
<i>Aree esterne per il ricovero</i>
E' possibile che gli spazi interni alla struttura non siano sufficienti o sufficientemente sicuri a seguito dell'emergenza, è quindi fondamentale stabilire dove poter alloggiare anche temporaneamente il materiale eventualmente danneggiato. Si consiglia perciò di individuare luoghi o di stipulare convenzioni per garantire l'alloggiamento temporaneo del materiale in caso di necessità presso strutture delle quali sia stata verificata l'idoneità, riportare qui una descrizione del luogo identificato e delle misure di protezione esistenti, una segnalazione dei requisiti dei locali e delle modalità di accesso del materiale archivistico o librario.
<i>Congelamento</i>
L'operazione di congelamento dei beni bagnati viene messa in atto al solo scopo di non far sviluppare muffe o funghi che li possano ulteriormente danneggiare. Tale operazione viene messa in atto quando le quantità dei beni bagnati è elevata e le forze/attrezzature disponibili non sono in grado di affrontare le conseguenze dell'evento, mettendo in atto rapide azioni di asciugatura. I criteri di congelamento devono altresì sottostare alle indicazioni di "ospitalità" (isolamento delle cassette su europallets mediante inserimento in cellophane isolanti che non permettano il contatto con eventuali elementi conservati nell'unità frigorifera ospitante) necessaria per il ricovero in celle disponibili ma destinate ad altro uso, di norma alimentare. Come già specificato le caratteristiche di imballo ed isolamento dei contenitori che conservano per il congelamento i beni bagnati, sono importanti al fine dell'accettazione all'interno di celle frigorifere destinate ad altro tipo di merci. Queste garanzie sono estremamente necessarie in caso di stipula di convenzione preventiva, per il rispetto delle prescrizioni interne delle imprese che gestiscono le celle

frigorifere. Indicare le informazioni utili e le operazioni da eseguire per la pianificazione dell'eventuale congelamento dei beni danneggiati, segnalare i contatti della società che si occupa del congelamento e dei luoghi di conservazione. Proseguire con le indicazioni fornite nella fase PIANO DI RIPRISTINO.
<i>Criticità</i>
Si riportano criticità possibili o riscontrate relative ai punti precedenti che potrebbero portare a problemi di cui tenere conto durante l'emergenza.
<i>Personale volontario di riferimento</i>
Coinvolgere del personale volontario solo previa formazione dello stesso o verifica delle qualifiche e delle competenze (verificare anche l'ente formatore stesso). Valutare e concordare le tempistiche di attivazione dei vari gruppi. Formalizzare delle convenzioni di collaborazione. Per quanto riguarda il personale volontario è necessaria una azione di controllo preventiva ed in corso d'opera affinché sia garantita la sicurezza dell'area di prelevamento e trattamento del materiale movimentato, tutto ciò per evitare inserimenti di elementi che hanno come fine il prelievo doloso di beni sfruttando la confusione naturale conseguente agli eventi . Utili sono i gruppi di volontariato costituiti e precedentemente vagliati che ab origine garantiscano e si prendano la responsabilità della gestione dei propri volontari, anche a livello assicurativo.
<i>Pianificazione economica</i>
Pianificazione preliminare delle risorse finanziarie da impiegare per le emergenze.
<i>Sistema di sicurezza durante l'intervento</i>
Approntare un sistema per la vigilanza e salvaguardia dei beni durante le fasi di intervento iniziale e lo stoccaggio. Quando gli ambienti colpiti da evento sono facilmente accessibili dall'esterno, o le operazioni di prelevamento e di salvaguardia si svolgano all'esterno del perimetro di protezione dell'edificio, è estremamente necessario costituire una "cintura sanitaria" messa in atto da personale fidato/volontari che impediscano l'avvicinamento a individui non autorizzati e vigilino sull'area, per impedire l'uscita fraudolenta di beni danneggiati e non.

PRE - PIANO DI RISPOSTA ALL'EMERGENZA

Questa sezione di Piano propone delle soluzioni operative per fronteggiare il cosiddetto “rischio residuo”, ovvero quello che non si è riusciti a ridurre con le attività stabilite nelle precedenti indicazioni, legato a eventi imprevedibili e imm modificabili.

Quelle fornite sono da considerarsi come indicazioni di massima, da adattare al caso specifico, alle sue particolari necessità, condizioni e risorse; si riferiscono ai soli tre rischi più comuni e importanti per i beni cartacei (allagamento, incendio, sisma).

È bene tenere presente ad ogni operazione che potranno verificarsi delle perdite: le scelte da compiere devono avere però come fine - il più possibile - l'annullamento di questa eventuale conseguenza.

Si introducono due interventi possibili per recuperare e ripristinare il materiale danneggiato (congelamento, liofilizzazione o asciugatura), per i quali si espongono vantaggi, criticità e standard da considerare già nelle prime fasi di intervento, al fine di rendere i beni destinati a questi trattamenti, il più adatti possibile.

E' utile considerare in fase di costruzione del PRE che l'addestramento del personale interno che si occupa dell'applicazione del medesimo sia messo in atto. Tutto ciò anche per attenuare se non annullare gli effetti emotivi che qualsiasi tipo di evento distruttivo o minaccia possa ricadere sugli operatori destinati alla salvaguardia dei beni. La raccolta di informazioni immediate, la loro valutazione e la risposta da effettuare conseguente, secondo i piani stabiliti, debbono essere prese con calma senza isterismi ed azioni concitate che complicherebbero solamente le azioni previste ed i risultati. Tutto ciò rispettando la catena di comando stabilita che parte dal direttore/responsabile del PRE o suo delegato.

INFORMAZIONI PRELIMINARI

In funzione dell'individuazione dei rischi individuati ed analizzati nelle precedenti sezioni, si riportano ora le azioni da intraprendere per rispondere al verificarsi delle possibili emergenze, suddivise per tipologia (alluvione/allagamento, incendio, sisma).

La compilazione è guidata e arricchita da esempi e buone pratiche.

Sarà quindi necessario:

- descrivere le procedure di intervento relative a ogni scenario di rischio insistente sullo specifico archivio/biblioteca,
- annotare punto per punto la catena di attività da eseguire e schematizzazione,
- attribuire compiti al personale, scelta degli interventi,

Per approfondimenti più dettagliati c.f.r. RIFERIMENTI del presente documento. Precedono queste schede una serie di informazioni generali e vevolevoli per ogni condizione emergenziale. È bene ricordare in questa sede che la risposta all'emergenza va necessariamente progettata in conseguenza alle valutazioni preliminari, in proporzione all'evento e alle risorse disponibili (le forze e le strutture presenti sono sufficienti?). In questo senso, le soluzioni di seguito proposte, sono da intendersi come una traccia da adeguare ad ogni situazione specifica.
<i>Vie di fuga</i>
Accertarsi della presenza di queste informazioni in piani sovraordinati, in caso presenti riportarle e verificarne l'adeguatezza anche rispetto alle condizioni sito ed evento specifiche. Lasciare sempre libere le vie di fuga e di calpestio anche fra le scaffalature, eliminare ogni possibile ostacolo lungo corridoi e percorsi di avvicinamento agli scaffali²⁰.
<i>Vie sicure per accesso mezzi</i>
Accertarsi della presenza di queste informazioni in piani sovraordinati così che siano coerenti ed inoltre già valutate, in caso siano già presenti riportarle e verificarne l'adeguatezza anche rispetto alle operazioni previste in caso di questo tipo d'emergenza.
<i>Localizzazione delle centrali degli impianti</i>
A fini cautelativi verificare la localizzazione delle centraline degli impianti: qualora il danno sia di origine idrica è sempre meglio staccare l'energia elettrica e quindi prima di entrare nei luoghi colpiti conoscere l'esatta posizione del quadro elettrico e quale interruttore staccare. Chiudere l'acqua avendo già verificato in fase di stesura del PRE la posizione della valvola di intercettazione ed il suo corretto funzionamento. Eseguire una periodica manutenzione degli impianti come metodo di efficace prevenzione di possibili danni e malfunzionamenti.

²⁰ Viene fatto riferimento ad una sentenza della Cassazione a sostegno di quanto sopra.

«Corte di Cassazione - Penale Sezione III - Sentenza n. 39360 del 30 settembre 2015 – u.p. 4 febbraio 2015 - Pres. Squasoni – Est. Andronio – Ric. C.D.. - Lo scopo di tenere sgombre da materiali le vie di circolazione non è tanto quello di assicurare una circolazione in una situazione di normalità ma una normalità di circolazione e una sicura via di fuga in una situazione di eccezionalità o di pericolo».

Viene data dalla Corte di Cassazione in questa sentenza una interpretazione sull'obbligo imposto dalle disposizioni di legge in materia di prevenzione infortuni di cui all'art. 64, comma primo, lett. b) del D.Lgs. 9/4/2008 n. 81 di assicurare che le vie di circolazione che conducono ad uscite o ad uscite di sicurezza siano sgombre da materiali. Lo scopo della norma, ha infatti precisato la suprema Corte, non è tanto quello di assicurare una circolazione in una situazione di normalità ma di consentirne l'utilizzazione in ogni evenienza e quindi di assicurare una normalità di circolazione soprattutto in situazioni di eccezionalità o di pericolo, in modo che, in caso di emergenza, siano sempre percorribili agevolmente le eventuali vie di fuga.

<i>Aree sicure</i>
Per raggruppamento personale e ammassamento materiali. Segnalazione di aree precedentemente individuate e destinate per il triage e materiali.
<i>Aree per il triage</i>
Segnalare l'area sicura dove sarà possibile eseguire il triage (fase di smistamento del materiale in base a tipologia di danno subito e di intervento richiesto). Funzione di norma espletata da un restauratore conservatore o da personale specificatamente addestrato.
<i>Aree di primo intervento</i>
Segnalare i locali protetti dove sarà possibile eseguire le prime operazioni di intervento, che abbiano una area tale da poter trattare comodamente i beni danneggiati in maniera lieve e che siano facilmente raggiungibili.
<i>Verificare disponibilità materiali</i>
Verificare la disponibilità dei materiali utili per il salvataggio dei beni (c.f.r. PIANO DI ANALISI DELLE RISORSE PRESENTI E ATTIVABILI IN CASO DI EMERGENZA), come buste di plastica, cassette di plastica, carrelli, ...
<i>Responsabili</i>
Riportare i nomi degli addetti alla sicurezza e le loro mansioni specifiche: referente e suo sostituto, squadra di emergenza, addetto alle relazioni con l'esterno. Bisogna ricordare che in caso di emergenza e sua risposta un solo referente deve avere relazione con chi interviene in aiuto come i Vigili del Fuoco o la protezione Civile e la catena di comando così a discendere, per evitare accavallamenti o incomprensioni inutili. Riportare i contatti di eventuali restauratori/ditte esterne già selezionati, che si occupano normalmente delle operazioni di restauro e conservazione. La documentazione a corredo del PRE come planimetrie con segnalate le vie di fuga e di evacuazione del materiale, impianti e collocazione topografica dei beni di primo prelievo, deve essere sempre a disposizione degli organi competenti alla salvaguardia (VVFF) e del responsabile dell'Emergenza dell'Istituto colpito dall'evento. La documentazione quindi va conservata in luogo raggiungibile e sicuro, sarebbe auspicabile averne una copia ulteriore depositata in altro luogo.
<i>Vigilanza</i>
Istituire un sistema di vigilanza durante le fasi di prelievo, intervento e stoccaggio. Il cosiddetto "cordone sanitario" viene istituito perché in fase di disastro si possono verificare asportazioni dolose di beni. Il

personale che interviene deve essere controllato è comunque necessario prestare attenzione per la sicurezza dei beni movimentati.

Parametri da considerare per successivo congelamento del materiale²¹

Come già indicato lo scopo del PRE è il recupero materiale dei beni vittime di disastro idrico qualora per dimensioni o per mancanza di personale non si possano mettere in pratica le operazioni di recupero entro le 48 ore si debbono congelare i beni.

Nel caso si opti per il congelamento di alcuni soggetti è necessario considerare preliminarmente:

- se esistano accordi con ditte per il congelamento e lo stoccaggio,
- verificare i costi per lo stoccaggio nel tempo,
- procurarsi materiale specifico (da considerare nel Piano delle Misure di Prevenzione, come pallet, teli di plastica, etc),
- provvedere all'isolamento dei pallet, soprattutto a fini igienici se la ditta di congelamento si occupa anche di materiale alimentare, ad esempio,
- altro...

Parametri da considerare per successiva liofilizzazione del materiale

Verificare preliminarmente:

- presenza di centro disponibile e qualificato (o replicabilità in centro con dotazione strumentale che si occupa di altro) e di accordi preesistenti,
- costi calcolati in funzione dei tempi di realizzazione del processo,
- mantenere uno spessore massimo delle buste (mantenendo unità documentale) in modo tale da garantire tempi ragionevoli per la liofilizzazione,
- prevedere l'utilizzo di distanziali tra le cassette,
- predisporre anche in anticipo un supporto rigido per il materiale (possibilmente già nelle buste di plastica),
- altro...

²¹ Il congelamento ha anche lo scopo di dilazionare i tempi di intervento e di recupero dei beni bagnati. Pur essendo la liofilizzazione un ottimo metodo di asciugatura ed in parte di disinfezione, è anche possibile asciugare poco alla volta il materiale congelato in ambienti idonei o con macchinari ad asciugatura forzata. L'imbustamento dei beni consente questa operazione prelevando di volta in volta la quantità di beni su cui si può intervenire. Sia per le operazioni di liofilizzazione che di asciugatura forzata l'imbustamento di piccole quantità di materiale è consigliabile in quanto facilita enormemente le operazioni di cui sopra.

RISCHIO ALLAGAMENTO
<i>Allerta</i> Seguire le procedure di allerta e contattare i responsabili interni ed esterni alla struttura. L'ingresso e quindi l'intervento sui beni sarà possibile solo al termine dell'intervento delle autorità e se la struttura verrà giudicata sufficientemente sicura. Il tempo dell'intervento degli esperti potrebbe essere utilmente utilizzato per organizzare le squadre.
<i>Vigilanza</i> Allarmare le squadre addette alla vigilanza. Ogni operatore è comunque tenuto a rivestire questo ruolo.
<i>Verificare l'origine dell'acqua</i> • da tubazione: tubazione in pressione (anche proveniente da impianti termici)/tubazione a caduta • evento atmosferico: flash flood, esondazione fiumi, tracimazione rete fognaria • acqua "effimera": termine creato ad hoc in questa sede, per indicare l'acqua assorbita dai beni posti in ambienti allagati e quindi con una Umidità Relativa (U.R.) molto elevata, non toccati direttamente dall'acqua e che si presentano come "finti asciutti"; l'ambiente subisce un forte innalzamento del valore igrometrico facendo assorbire più acqua da umidità relativa di quanta normalmente ve ne sia in ambiente, provocando lo sviluppo postumo non previsto di muffe e funghi.
<i>Interrompere il flusso d'acqua se di origine impiantistica</i> Chiudere il rubinetto centrale dell'impianto idraulico. Verificarne in fase preliminare la collocazione e il funzionamento, verificare la presenza di valvole esterne della rete.
<i>Disinserire la corrente elettrica</i> Soprattutto se si è i primi ad accorrere sul luogo del disastro: l'acqua è un ottimo conduttore di corrente e si crea il rischio di folgorazione per gli operatori.
<i>Munirsi di sistema di illuminazione alternativo/portatile</i> Soprattutto nel caso sia stata tolta per precauzione la corrente.
<i>Primo sopralluogo</i> Eseguite le procedure di evacuazione e messa in sicurezza del personale. Al termine dell'intervento specialistico, sarà possibile rientrare nell'edificio. A questo punto eseguire un primo sopralluogo per valutare la situazione e lo stato dei beni. Registrare le condizioni generali e particolari con l'aiuto di un rilievo fotografico anche per i fini

assicurativi prima di eseguire l'intervento di salvaguardia.
<i>Briefing</i>
Con il responsabile del PRE, il direttore e tutti i responsabili delle unità intervenute è utile organizzare le azioni, prendendo visione dei luoghi sottoposti a danno, degli spazi disponibili, della possibilità di intervento e dell'entità del danno. Questo momento iniziale è necessario per evitare azioni sovrapponibili ed inutili conseguenti dispersioni di forze, inutili isterismi e perdita della visione della realtà. Solo in casi eccezionali, con acqua ascendente se possibile ed autorizzato dai VVFF si può procedere con celerità al prelievo dei beni in pericolo di allagamento prima di aver pianificato gli interventi previsti. La calma è l'aiuto maggiore. Risulta importantissimo garantire l'accesso degli operatori di risposta all'emergenza ai contenuti del Piano e alle indicazioni del Piano di Risposta all'Emergenza.
<i>Risanare l'ambiente</i>
Eliminare l'acqua dagli ambienti (con l'utilizzo di pompe o aspira liquidi) facendo attenzione che i cavi di alimentazione delle pompe o degli aspira liquidi non siano a loro volta a contatto con l'acqua, asciugare il più possibile i pavimenti.
<i>Affidare ai componenti della squadra specifiche mansioni</i>
Compilatore scheda: la scheda di accompagnamento dei beni impacchettati è necessaria qualora i dati di catalogazione o di inventario del bene non siano rilevabili per il distacco del cartellino o il dilavamento degli inchiostri. E' necessario monitorare i beni nel loro destino in modo da controllare ed evitarne la perdita. Il problema si presenta quando si tratta di carte sciolte sparse raccolte in un area definita (o indefinita) che devono qui sì obbligatoriamente contenere i dati essenziali per identificare i beni nel loro percorso, pertanto la scheda con i dati essenziali dovrà essere compilata. Dovrà essere aggiunto all'interno del sacchetto destinato al congelamento ed alla eventuale liofilizzazione un numero progressivo scritto a matita (non direttamente sul bene prelevato) che riporti poi in un registro generale il numero di beni inviati al congelamento e quindi fuori dall'istituto. Questo codice dovrà riferirsi all'evento calamitoso, alla squadra di soccorso, al tipo di danno e al luogo in cui il bene verrà inviato per lo stoccaggio. Schede troppo complicate o lunghe da compilare sono un ostacolo al fluente proseguo delle operazioni ed a rischio di dispersione nelle operazioni successive. Si fa comunque riferimento alla scheda ministeriale di descrizione dei beni prelevati ed inviati ad altro luogo di stoccaggio/lavorazione, che è compilabile a discrezione del responsabile del PRE.

- prelevatore,
- trasporto,
- vaglio (triage): operazione che deve svolgere un restauratore conservatore o personale debitamente formato e che destinerà i beni secondo le forze, le disponibilità e proporzionalmente alla quantità di beni danneggiati.
- impacchettamento
- oppure
- destinazione diretta al trattamento (se si dispone di locali adeguati).

La programmazione delle attività deve prevedere una giusta spartizione tra i vari componenti della squadra considerando che più ruoli possono essere svolti dalla medesima persona, considerando il carico di lavoro cui è sottoposta. Si ritiene necessario a questo scopo programmare delle turnazioni o delle pause.

Verifica dell'inventario topografico

Analizzare l'inventario topografico, in modo da verificare, in base al codice di urgenza attribuito, dove siano posizionati i materiali da salvare prioritariamente. Programmare i salvataggi conseguentemente.

Estrazione del materiale

Seguire le priorità indicate nell'inventario topografico.

Si tratta di un'azione molto delicata, il materiale bagnato potrebbe distruggersi.

Il materiale cartaceo aumenta di volume e di peso quando bagnato: se si dispone di scaffali aperti meglio non riempire – preventivamente - completamente i ripiani, in modo da lasciare un po' di agio ai beni e facilitarne nonostante l'eventuale aumento di volume, l'estrazione.

Ricordarsi che i beni bagnati se rilegati hanno perso consistenza, che gli adesivi si sono attenuati e che i supporti sono molto più deboli. Così anche per i beni composti da carte libere in faldone o busta nel quale i lacci di chiusura potrebbero fare effetto sega sulle carte.

I beni pertanto dovranno essere estratti ponendo una mano sul taglio anteriore del bene (dalla parte opposta al dorso visibile) e prendendo con l'altra mano il bene per il dorso, in modo da avere due punti di contatto ed estrarlo con cautela. Evitare il più possibile l'attrito con gli altri beni bagnati in modo da non deformare o asportare le parti non più aderenti e solidali.

Particolare attenzione va posta per i beni contenuti nei compactus, vanno estratti tutti i beni anche quelli non danneggiati o bagnati, in quanto i compactus potrebbero divenire camere climatiche che favoriscono lo sviluppo di muffe. Questo fino all'accertamento di condizioni igrotermiche stabili e favorevoli.

Dalla quantità di materiale danneggiato dipendono le scelte sulle azioni da intraprendere successivamente.

1. Prelevare successivamente dalle scaffalature secondo l'ordine sequenziale stabilito i beni, posizionandoli in contenitori rigidi in plastica forata (tipo cassette della frutta), evitare carichi eccessivi.
2. I beni totalmente sommersi non hanno la priorità di essere prelevati per primi salvo che abbiano inchiostri o colori solubili.
3. Prelevare prioritariamente quelli a rischio immediato di immersione o di assorbimento dell'acqua e successivamente gli altri, considerando eventualmente le specifiche decise ed indicate nel topografico.
4. Depositare i beni in cassette di plastica traforata per evitare il più possibile la manipolazione, i beni vanno posti in piano mettendo sotto il/i più largo senza caricare troppo la cassetta e facilitarne il trasporto, facendo attenzione che nulla strabordi dalla cassetta o ne superi il volume.
5. Accompagnare ogni contenitore con il numero o la scheda che stabilisca anche da dove – topografico - sono stati prelevati i beni.

Triage

Questa operazione, da svolgersi in ambiente sicuro in presenza delle attrezzature minime per i primi interventi, per l'impacchettamento preliminare al congelamento, ecc.. Serve a distinguere per categoria di livello di danno i beni colpiti e a determinarne di conseguenza le priorità e tipologie di intervento.

1. Consegnato il contenitore al punto di raccolta procedere alla selezione del materiale secondo le tipologie di danno:
 - bagnato;
 - bagnato per circa il 20%;
 - umido e/o presunto asciutto²².

²² La definizione presunto asciutto stabilisce lo stato di attenzione a cui deve essere sottoposto un bene dopo un'emergenza da acqua, durante la quale pur non essendo stato bagnato direttamente, a causa dell'innalzamento dell'umidità relativa ambientale, può presentare anch'esso un assorbimento di umidità tale da poter sviluppare in seguito muffe e conseguente degrado dei costituenti, manifestare alla manipolazione l'indebolimento dei supporti, degli adesivi e delle legature.

I pavimenti ed i muri degli ambienti allagati nei giorni successivi possono restituire quanto assorbito e quindi il ripristino dei locali dovrà tenere conto anche di questo fattore non percepibile senza un rilevamento strumentale.

Lo stato di presunto asciutto si risolve quando dopo attento monitoraggio per i giorni seguenti il bene manifesta una umidità relativa idonea alla sua durata. Gli ambienti colpiti da emergenza acqua o da umidità ambientale elevata e costante (ad esempio i seminterrati) devono, prima di riospitare i beni tolti durante l'emergenza, presentare caratteristiche ambientali costanti ed adeguate per la conservazione (45%-65% U.R. ; max 18 – 20°C). Lo stato di presunto asciutto è uno stato di attenzione costante specialmente

Qualora la quantità di materiale bagnato non sia affrontabile dal personale e dalla logistica, si procederà all'impacchettamento e al congelamento.

2. Inserire in sacchetti di cellophane i beni bagnati da inviare al congelamento, comporre piccoli pacchi e uniformando il più possibile le dimensioni. Accompagnare dal numero o dalla scheda inserita all'interno e sigillare. Piccoli pacchetti permetteranno una asciugatura più rapida con minori costi. È necessario sgrondare il più possibile i beni se possibile comprimendoli con delicatezza. Tale operazione da svolgersi con cautela faciliterà notevolmente le fasi successive di asciugatura.
3. Evitare accuratamente compressioni e deformazioni dei beni, per i beni presunti asciutti o leggermente bagnati porli in contenitori idonei al trasporto, questi possono essere anche appoggiati sul dorso. Facendo comunque attenzione ai carichi in modo da non rendere troppo pesanti i contenitori ed affaticare gli operatori, ed inoltre rendere difficoltoso e pericoloso il trasporto delle cassette.
4. Per i soli beni archivistici - sistemare le cartelle, poste sempre in sacchetti, in piano avendo cura di alternare i dorsi delle cartelle qual'ora si sia costretti ad impilarne più di una,
5. Evitare che i contenitori impilabili abbiano al loro interno involucri sporgenti, in modo da non comprimerli accidentalmente o produrre ulteriori danni.
6. Riempire gli eventuali spazi vuoti nei contenitori con cartoni da imballo o carta o altro disponibile per evitare che il materiale confezionato e depositato poi su europallets si sposti provocando deformazioni o danni ulteriori.
7. Ogni contenitore deve riportare un'etichetta (ALLEGATO 3 – ETICHETTA CASSE) con la specifica della tipologia di danno.

Materiali da congelare

8. Inviare al più presto il materiale bagnato e già confezionato al congelamento avendo cura di registrare accuratamente cosa va e dove.
9. Entro 6 ore volumi in carta patinata (che ha bisogno di particolare attenzione con il sostegno di esperti. Se la carta patinata si sta già asciugando potrebbe essere necessario reumidirla questo per evitare che la patinatura aderisca in fase di asciugatura non monitorata), entro le 48 ore il resto.

nelle condizioni di emergenza quiescente dove i locali umidi e raramente frequentati manifestano a lungo andare le stesse conseguenze di un allagamento.

10. Particolare attenzione va posta per il materiale membranaceo sul quale dovrebbero essere immediatamente poste in essere le procedure di recupero da parte di un restauratore.
11. Altra particolare attenzione per le coperte in cuoio.
12. i beni membranacei devono andare alla liofilizzazione solo con garanzie da parte dell'operatore ed esclusivamente per i volumi o i registri. Bisogna comunque prestare attenzione ai beni con coperte in cuoio o pergamena che necessitano preferibilmente di particolari attenzioni e vanno trattati separatamente da personale specializzato con un percorso dedicato e subito nelle 48 ore seguenti l'evento accidentale. Sui beni totalmente membranacei si deve intervenire al più presto, operazioni che vengono eseguite da parte di restauratori. Una ulteriore e particolare attenzione va posta alle pergamene sigillate o con sigilli pendenti.

Materiale bagnato

I beni bagnati in piccola parte, dovranno essere inviati nel luogo individuato per le operazioni di asciugatura, avendo cura di metterli in contenitori valutando le stesse modalità o cautele di quelli bagnati, sempre con la scheda o numero al seguito e con la registrazione da parte del responsabile o di suo delegato di cosa va e dove.

Se i beni sono sporchi di fango vanno lavati con acqua corrente pulita per evitare incrostazioni difficili da rimuovere successivamente (bisogna prevedere anche in un ambiente allagato la possibilità d'uso di acqua pulita usando un tubo di gomma in luogo apposito).

Rimuovere l'eccesso d'acqua con una leggera compressione del bene e proseguire con le operazioni necessarie: invio al congelamento o al trattamento.

N.B. le operazioni di cui sopra ed al seguito devono essere eseguite o da personale specializzato o sotto la vigilanza di quest'ultimo.

La quantità di materiale che verrà congelato dipende fortemente dalle risorse messe in campo e anche dalle necessità.

Altri materiali

Beni di altra natura materica come tavole dipinte, tele, stoffe, statue e legni policromi, etc. devono essere trattati obbligatoriamente in tempo breve solo da un restauratore certificato.

Altri materiali come CD, videocassette, microfilm, supporti magnetici devono essere trattati in rispondenza alle specifiche caratteristiche materiche, di uso e di degrado subito. Si rimanda ad una letteratura più dettagliata di settore per questo tema, ricordando comunque che:

- le copie eliografiche e i lucidi possono essere asciugati immediatamente sia all'aria, sia congelati,

- le stampe fotografiche se non è possibile intervenire subito facendole asciugare appoggiate sul verso, vanno interfogliate con carta siliconata prima dell'eventuale congelamento e comunque nei tempi di intervento vanno tenute umide per evitare che le emulsioni si secchino ed aderiscano alle altre. E' auspicabile una asciugatura in ambiente e solo qualora la separazione delle fotografie dal resto dei documenti o dall'album sia estremamente difficoltosa si può procedere alla liofilizzazione, possibilmente prima con un campione per osservare i risultati.
- i negativi fotografici e le pellicole non possono essere congelati, ma possono essere lavati con acqua fredda e posti ad asciugare all'aria con il lato emulsione verso l'alto,
- i nastri magnetici e i CD non possono essere congelati, ma lavati con acqua fredda e posti ad asciugare all'aria con il lato di registrazione verso l'alto.

Operazioni da eseguire su beni trattabili direttamente

I beni bagnati parzialmente che si possono trattare in spazi destinati a questa operazione nell'arco delle 48 ore, su di essi si possono eseguire le seguenti operazioni:

- preparare il piano di lavoro : tavolo, pavimento con telo di plastica, carrelli, ecc...
- Se possono stare verticali senza causare deformazioni, i beni rilegati si appoggiano sul piano dalla parte asciutta aprendoli a ventaglio, avendo cura di non perdere segnature o cartellini al seguito che identifichino il bene. Sottoporre l'ambiente dove sono collocati i beni ad asciugatura forzata; non innalzare la temperatura ambiente ed utilizzare batterie di deumificatori. Non esporre al sole i beni da asciugare! Controllare sempre l'eventuale sviluppo di muffe non presenti prima. Non riempire eccessivamente i locali destinati ad ospitare i beni che si possono asciugare in quanto l'umidità da asportare sarebbe troppo elevata e quindi con tempi lunghi che possono permettere il manifestarsi di muffe. I criteri di asciugatura in ambiente con ventilazione secca forzata vanno valutati secondo il grado di inumidimento dei beni potenzialmente asciugabili con questo metodo.
- Se necessaria interfoliazione, bisogna fare attenzione a separare le pagine cercando un punto asciutto che faciliti l'operazione, inserire frequentemente dei fogli assorbenti (asciugoni, carta in rotolo, ecc...) i quali dopo al massimo qualche ora circa debbono essere sostituiti magari cambiando punto d'inserimento. Fare attenzione che le pagine bagnate fra di loro producono un effetto ventosa ed è frequente che si lacerino all'apertura. Non esagerare nell'interfoliazione in quanto grandi quantità di carta assorbente deformano il volume/registro provocando ulteriori danni.

Da esperienze pregresse è stato stimato che il lavoro di interfoliazione per una quantità di

materiale bagnato pari a 1 metro lineare richiede il lavoro di un operatore per 20 giorni (sino a completa asciugatura e che lo spazio appena sufficiente per svolgere questa attività corrisponde a circa 1 m² di piano di lavoro. Si può interrompere l'interfoliazione quando il volume ha ridotto notevolmente la quantità di acqua e si può porre verticalmente su un piano, aperto a ventaglio.

È rischioso, in linea di massima da evitare, interfogliare: miniature, materiale membranaceo, carta patinata.

Grandi formati

I grandi formati come i manifesti per esempio, devono essere stesi per poter essere asciugati o in casi eccezionali appesi dalla parte asciutta ad un filo – ma solo se la parte umida non rischia lacerazioni. Le mappe telate dovranno subire un trattamento ad hoc.

Prelievo dei grandi formati o di beni in rotolo appoggiandoli su "barelle" (fogli di poliuretano, polistirolo, compensato plastificato, ecc...) rigide - condotte da due persone- evitando accuratamente il trasporto dei beni a mani libere. Questa tipologia di materiale ha bisogno di una cura particolare perché facilmente, come intuibile, potrebbe ricevere un ulteriore e grave danno dalle fasi di salvataggio.

Attenzione

Cosa NON fare durante l'emergenza:

1. NON impilare i libri o beni archivistici bagnati o molto umidi così da evitare compressioni o deformazioni dannose, attenzione a borchie o parti metalliche sporgenti,
2. NON aprire i libri o i registri bagnati se non per le operazioni di asciugatura,
3. NON pressare - se non con cautela e solo per lo sgrondo dell'acqua in eccesso,
4. NON sfregare,
5. NON rimuovere copertine o cartelle bagnate; le uniche cartelline che possono essere rimosse ma non scartate – debbono essere collegate ai documenti contenuti sono quelle colorate che si decolorano a contatto con l'acqua, dalle quali migrano i colori sui documenti spesso non eliminabili in fase di restauro/recupero. Eventualmente in fase di separazione delle cartelle colorate bagnate riportare se presenti , numeri di collocazione, pratica, altro, utile alla lettura del bene. Operazione che va attentamente valutata dai responsabili delle operazioni,
6. NON separare le pagine se non per l'interfoliazione qual'ora sia possibile e necessaria,
7. NON scrivere su carta o libri bagnati,
8. NON usare sui libri danneggiati pinze, graffette, adesivi,
9. NON usare carte assorbenti colorate o con inchiostri.

In presenza di compactus

I compactus pur avendo un evidente vantaggio, in caso di evento dannoso possono scorrere con difficoltà sui binari, non hanno una apertura tale da permettere che tutti i moduli abbiano una circolazione d'aria idonea e non sono stagni.

L'acqua può riuscire comunque ad entrare, una volta dentro "gonfia" il materiale cartaceo, potrebbe essere quindi molto difficile se non impossibile estrarre senza danni ulteriori i beni contenuti (questo vale anche per gli scaffali aperti). A causa dell'insufficiente possibile circolazione d'aria devono essere svuotati, verranno poi riempiti solo quando i beni sono sicuramente asciutti ed i locali sono tornati a valori termo igrometrici stabili ed idonei.

È comunque utile un servizio di monitoraggio ulteriore per i depositi con compactus (ma non solo). Vale come per gli scaffali il principio del riempimento "attenuato", lasciando un po' di spazio tra i beni in modo tale da diminuire il rischio di compressione a seguito dell'aumento di volume provocato dall'acqua.

È necessario che vi sia un controllo dell'umidità dei beni ritenuti asciutti prima di ricollocarli sui piani di conservazione. Lo stesso vale per i locali che hanno subito il danno da acqua. La misurazione dell'umidità relativa dei locali deve rilevare una idoneità ed una costanza tali da non rivelare il rilascio di umidità dai pavimenti e dai muri che possono aver assorbito copiosamente l'acqua e quindi restituirla nelle settimane successive. Se l'evento dannoso avviene in un periodo climaticamente piovoso o molto umido il monitoraggio dei locali ripristinati prima del ricollocamento e del ripristino delle attività deve essere massimo.

Conseguenze di un'asciugatura incompleta o inefficace

- possibile sviluppare agenti patogeni (ad esempio muffe) sui beni conservati, dannose anche per la salute degli operatori,
- aumento dei costi e dei tempi di recupero,
- possibilità di recupero,
- compattamenti che rendono impossibile la consultazione di tutte le pagine.

RISCHIO INCENDIO

Per quanto riguarda la normativa antincendio si rimanda a quanto disposto dal D.P.R. n. 151 del giorno 1 agosto 2011. Sono soggetti alle visite e ai controlli di prevenzione incendi i depositi contenenti quantitativi di carta superiori ai 5.000 Kg e gli immobili tutelati ai sensi del D.Lgs. 42/2004 e s.m. destinati alla conservazione di archivi o biblioteche.

La conseguenza più impattante da considerare in caso di incendio, riguarda la presenza di acqua da spegnimento: in questo caso è necessario eseguire tutte le operazioni descritte e stabilite per la reazione al

RISCHIO ALLAGAMENTO

In assenza di acqua invece, si ha più tempo per progettare un intervento adeguato. Questa scelta va valutata da personale specializzato.

Ci si raccomanda di provare a contrastare il fuoco solo se:

- l'incendio ha dimensioni circoscritte,
- si hanno vie d'uscita libere,
- si dispone di mezzi ed attrezzatura adeguata,
- il personale è stato debitamente formato.

Al contrario, si invita a non agire se:

- non si è sicuri dei propri mezzi,
- l'incendio si sta espandendo oltre l'area iniziale,
- può impedire l'accesso alle vie d'uscita.

Gli incendi che possono verificarsi in archivi e biblioteche sono considerati di classe A, ovvero riguardanti tutti i materiali solidi a base cellulosica quali il legno, la carta, i tessuti e quelli a base organica come cuoio e pergamena. Questi materiali sono soggetti a due tipi di combustione: una vivace, caratterizzata da fiamme e un'altra priva di fiamme visibili, lenta e quasi "covante", caratterizzata dalla formazione di braci, ma non meno pericolosa e molto insidiosa in quanto non immediatamente individuabile²³.

La combustione produce ceneri costituite da vari prodotti mescolati con materiali incombusti che in parte

si disperdono nell'aria trasportati dai gas (fumo). Il calore, le ceneri, i fumi e la fuliggine provocano danni ai supporti scrittori e alle mediazioni grafiche.²⁴

Allerta

Seguire le procedure di allerta e contattare i responsabili interni ed esterni alla struttura, Vigili del Fuoco in primis.

Solo se non è presente un impianto estinguente dedicato e se l'incendio è di piccolissime dimensioni intervenire con i dispositivi a disposizione (estintori, manichette per l'acqua, etc) – va considerato che l'incendio va spento tenendo presente la salvaguardia delle persone presenti e di ridurre al minimo il danno dei beni materiali. Può essere utile se possibile contenere piccole fiamme con gli strumenti a disposizione in attesa dell'arrivo dei VVFF.

Qual'ora vi sia stata evacuazione l'ingresso e quindi l'intervento sui beni sarà possibile solo al termine dell'intervento delle autorità e se la struttura verrà giudicata sufficientemente sicura.

Il tempo dell'intervento degli esperti potrebbe essere utilmente utilizzato per organizzare le squadre.

Vigilanza

Allarmare in contemporanea alla scoperta dell'evento le squadre addette alla vigilanza. Ogni operatore è comunque tenuto a rivestire questo ruolo.

Le operazioni successive sono da mettersi in pratica a fine evento quando vi è certezza di poter entrare nei locali interessati.

Interrompere l'erogazione del gas

A scopo precauzionale, qualora non sia già stato fatto.

Munirsi di sistema di illuminazione alternativo/portatile

Soprattutto nel caso sia stata tolta per precauzione la corrente.

Primo sopralluogo

Eseguite le procedure di evacuazione e messa in sicurezza del personale, al termine dell'intervento

²⁴ Oltre ai danni causati dall'acqua eventualmente utilizzata dai Vigili del Fuoco per l'estinzione, vanno considerate in fase di scelta preventiva dei sistemi di spegnimento mobili e fissi le possibili conseguenze dovute all'utilizzo di polveri estinguenti; alcuni test eseguiti nei laboratori dell'ICRCPAL nel 2008 (http://www.icpal.beniculturali.it/allegati/Estinguenti_polveri_k.pdf) hanno evidenziato in particolare che l'esposizione all'aerosol di polveri di potassio costituenti il compound estinguente comporta effetti dannosi, più o meno intensi e pressoché immediati sulla carta, sulla pelle e sulla pergamena. L'estrema micronizzazione delle particelle di aerosol rende estremamente difficile, se non impossibile, la rimozione meccanica del particolato depositato sul materiale documentario, di sua natura poroso, con la conseguenza che non è possibile evitare eventuali effetti dannosi a lungo termine.

specialistico, sarà possibile rientrare nell'edificio. A questo punto eseguire un primo sopralluogo per valutare la situazione e lo stato dei beni. Registrare le condizioni generali e particolari con l'aiuto di un rilievo fotografico.

Risanare l'ambiente

Se è presente acqua conseguente alle operazioni di spegnimento:

- eliminare l'acqua (con l'utilizzo di pompe o aspira liquidi), asciugare il più possibile i pavimenti,
- garantire ventilazione ed effettuare le prime operazioni per prevenire la formazione di muffe.

Danni conseguenti allo spegnimento

Le operazioni di spegnimento dell'eventuale incendio possono causare a loro volta ulteriori danni causati dal mezzo estinguente utilizzato, in caso di acqua riferirsi alla scheda precedente (RISCHIO ALLAGAMENTO) bisogna considerare che i beni che hanno parti combuste e poi bagnate sommano le conseguenze di due eventi già gravi se presi singolarmente, con l'aggiunta della diffusione delle ceneri nere che imbruniscono ulteriormente i supporti. La fragilità delle parti combuste richiederà una ulteriore cautela nella manipolazione soprattutto in fase di estrazione dai piani di appoggio se i beni si trovano ancora nella loro sede.

Nel caso di presenza di polveri estinguenti queste vanno aspirate con l'ausilio di aspiratori con filtri idonei ed eventuali leggere pennellature e/o insufflazioni d'aria. Queste operazioni vanno effettuate da personale particolarmente addestrato e che sappia quando si possono mettere in opera queste particolari azioni - in quanto si potrebbero ottenere danni notevoli dall'uso maldestro degli aspiratori, nonché possibili rischi per la salute degli operatori. I beni puliti per un po' di tempo vanno monitorati per verificare eventuali variazioni chimiche o biologiche dei supporti, soprattutto nei cuoi o nelle pergamene per eccessivo rinsecchimento o altro. L'asportazione delle polveri estinguenti non è comunque mai totale e per questo va vigilato perché le polveri non sono sempre così inerti.

Affidare ai componenti della squadra specifiche mansioni

- compilatore scheda, le considerazioni di questa mansione sono identiche precedentemente descritte per i danni da acqua;
 - prelevatore,
 - trasporto,
 - vaglio (triage):
 - impacchettamento
- oppure

- destinazione diretta al trattamento (se si dispone di locali adeguati)

Verifica dell'inventario topografico

Analizzare l'inventario topografico, in modo da verificare, in base al codice di urgenza attribuito, dove siano posizionati i materiali da salvare prioritariamente. Programmare i salvataggi conseguentemente.

Estrazione del materiale

Seguire le priorità indicate nell'inventario topografico. Prevedere che in caso di incendio le segnalazioni sulle scaffalature potrebbero andare distrutte e quindi predisporre in fase preventiva una piantina con le collocazioni di beni con precedenza di salvataggio.

Si tratta di un'azione molto delicata, il materiale può ulteriormente danneggiarsi.

Dalla quantità di materiale danneggiato dipendono le scelte sulle azioni da intraprendere successivamente.

1. Prelevare successivamente dalle scaffalature secondo l'ordine sequenziale stabilito i beni, posizionandoli in contenitori in plastica, evitare carichi eccessivi.
2. Accompagnare ogni contenitore con la scheda (ALLEGATO 1 - SCHEDA RILEVAZIONE DANNI)

Attenzione

Bisogna ricordare che un bene che ha subito un incendio è di norma annerito e con parti combuste particolarmente fragili, pertanto la manipolazione è necessariamente cauta. Qualora vi sia l'aggiunta di acqua da spegnimento le operazioni dovranno essere comprese in quelle determinate per il danno d'acqua.

I beni sicuramente non umidi vanno comunque imbustati o collocati in scatole o su ripiani protetti e manipolati il meno possibile, evitando sfregamenti di ogni tipo: potrebbe essere utile in questo caso l'utilizzo anche di buste di carta così da garantire eventuali traspirazioni del bene, o in subordine di un sacchetto di polietilene al quale eventualmente si è fatto qualche buco per evitare remote condense. Sempre comunque sotto attento monitoraggio durante il periodo di attesa di recupero.

L'idonea conservazione provvisoria permette di diluire i tempi di recupero secondo le necessità e le urgenze, applicando poi così le tecniche migliori per il restauro dei beni.

RISCHIO TERREMOTO

Le procedure da eseguire sono assimilabili a quelle precedentemente descritte, considerando che, nella maggior parte dei casi, il materiale archivistico sepolto da un crollo o da una frana subisce generalmente danni di tipo meccanico ed è pertanto recuperabile con un intervento sollecito ed accurato, ma sicuramente non di urgente esecuzione. Le tempistiche vanno calcolate in base al possibile innescarsi di problematiche conseguenti che esporrebbero i beni ad agenti esterni (acqua, ambiente, parassiti, contaminanti, ecc), come allagamento per rottura di tubazioni o per il crollo della copertura o crollo definitivo dell'edificio. L'accesso alle aree disastrose ed ai beni danneggiati od in pericolo è conseguente all'autorizzazione delle autorità competenti.

Qualora invece si sia verificata solamente caduta di materiale archivistico/bibliotecario dalla scaffalature le operazioni sono meno urgenti rispetto ai danni descritti in precedenza.

Le conseguenze del crollo da terremoto sono la deformazione dei beni, la rottura, la perdita di parti o frammenti, l'impolveramento, quindi, se il materiale non è particolarmente danneggiato, le operazioni di recupero dovranno essere determinate dal tipo di danno come l'asportazione delle polveri depositate, alla separazione di beni danneggiati per la soluzione del danno.

Le operazioni devono concentrarsi sul recupero di tutti i frammenti dispersi e riunirli in un sacchetto/scatola di contenimento in attesa di azione ripartiva/ restauro.

Risulta fondamentale in questi casi, soprattutto riguardo ad una certa tipologia di documentazione, possedere, nonché conservare anche in altra sede, - come peraltro già indicato - una descrizione dettagliata del posizionamento dei vari beni, in modo da agevolare l'eventuale recupero d'emergenza da parte delle forze di pronto intervento.

Va comunque considerato che, in caso di terremoto in quanto coinvolge molti edifici di un dato territorio, si verifichi una diffusa carenza di spazi per effettuare azioni di recupero e di ricollocazione temporanea: per rendere fruibile la documentazione è a questo scopo possibile programmare l'utilizzo di container, posti all'ombra e in aree sicure, con possibilità di ventilazione e sotto controllo per garantirne la sicurezza.

PIANO DI RIPRISTINO

Questa fase concerne le attività che temporalmente vengono eseguite successivamente a quelle di messa in sicurezza dei beni a seguito del verificarsi di un evento calamitoso e comprendono tutte quelle operazioni finalizzate a stabilizzare il materiale danneggiato per consentirne la ricollocazione e il riutilizzo.

Tra questi procedimenti includiamo:

- la **pulitura**, per cui vanno utilizzate attrezzature adeguate e personale specializzato,
- la **uplicazione**, per rendere disponibili, al di là dell'autenticità materica, almeno il contenuto di beni archivistici compromessi sul quale destino si deciderà, considerando che la duplicazione in digitale NON è una forma di conservazione, questa riguarda solo il documento in originale,
- lo **scarto**, da eseguirsi seguendo procedure normate e codificate,
- il restauro,
- la **liofilizzazione**, a cui questo lavoro dedica un breve approfondimento metodologico e pratico, supportato da una sperimentazione svolta da un gruppo di ricerca del Politecnico di Torino²⁵, in particolare dai prof. Davide Fissore e Antonello Barresi, che hanno redatto la scheda di seguito riportata.

²⁵ http://www.disat.polito.it/it/il_dipartimento/strutture_interne/laboratori_interni/laboratorio_di_liofilizzazione

Liofilizzazione - introduzione

(a cura di Paola Mussini)

Si è deciso di concentrare l'attenzione di questa parte del documento sulla **liofilizzazione** quale utile tecnica di ripristino, in quanto consente di ottenere ottimi risultati sul materiale cartaceo se adeguatamente progettata ed eseguita. La letteratura di settore²⁶ non offre molti riferimenti e si dimostra in alcuni casi lacunosa, talvolta poco precisa e discordante, molto spesso priva di un supporto di dati sperimentali a comprovare le tesi esposte. Pertanto si è deciso di condurre dei test su campioni di materiale cartaceo, in collaborazione con il team di ricerca del Politecnico di Torino che si occupa di liofilizzazione (e che ha curato la scheda successiva).

Gli esperimenti sono stati condotti nel mese di marzo 2016 su beni sani, appositamente bagnati in modo tale da poter registrare e misurare eventuali cambiamenti di forma, peso e struttura a termine del processo di liofilizzazione. Sono stati per questo motivo scelti dei campioni che potessero essere rappresentativi della maggior parte dei materiali presenti in un archivio/biblioteca, con particolare riferimento a quelli più "difficili" da recuperare, in modo da validare l'efficacia del processo e garantire di contenere ulteriori possibili danni.

A questo scopo sono stati selezionati beni di carta risalente all'epoca fascista, in quanto presenta una scarsa qualità, carte patinate, materiale membranaceo risalente a varie epoche, fogli in cartelline colorate.

I dati relativi ad ogni campione sono riportati nella seguente tabella:

²⁶ Per i riferimenti bibliografici sul tema vd sezione **Riferimenti - Liofilizzazione**

SOPRINTENDENZA ARCHIVISTICA e BIBLIOGRAFICA DELLA LOMBARDIA

Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche

A cura di Paola Mussini, Luciano Sassi – giugno 2016

CAMPIONE	NOME	DATA	CONDIZIONI DI PARTENZA					FINE PROCESSO	
			DIMENSIONI [cm]	PESO [g]	PESO [g]	Δ PESO	% PESO	DIMENSIONI [cm]	PESO [g]
1	Lucia di Lammermoor, libretto d'opera rilegato	1931	11,8x17,9x0,3	19,8	36,6	16,8	84,85	11,8x17,9x0,5	18,8
2	Agenzia Abram Lewis, volume rilegato a filza	1934	13x19,2x2,7	350,64	755	404,36	115,32	13x19,2x3	352
3	Brochure patinate, gruppo di 8	anni 90	21,1x29,5(28)x1	578,3	949,6	371,3	64,21	21,1x29,5(28)x2	556
4	Cartellina rossa con carta stampata	anni 90	24,5x33x1	396	876	480	121,21	24,5x33x3	382,4
5	Pergamena nuova	anni 2000	9,2x8	0,89	4,8	3,91	439,33	9,2x8	1,8
6	Pergamena con lacci	1580/1581	4,4x7	1,65	3,6	1,95	118,18	4,4x7	1,6
7	Prova di stampa	XVIII sec	12x8	0,58	1,9	1,32	227,59	12x8	0,65
8	Pergamena imbrunita	XIII/XVI	3,5x4,2	0,26	0,8	0,54	207,69	3,5x4,2	0,3
9	Coperta con pelle	XVI/XVII	9,5x16,3	27,1	53,3	26,2	96,68	9,5x16,3	23,7
10	I Proscritti, volume rilegato a filza	1943	13,4x19,5x2,2	393	788,8	395,8	100,71	13,4x19,5x3,8	410,7
11	Coperta di cartoncino (10K T10)	XVII sec	17,5x10,5	12,7	24,3	11,6	91,34	17,5x10,5	11,5
12	Carta con foxing	XVI sec	9,9x11,5	0,57	2,2	1,63	285,96	9,9x11,5	0,6
13	Cartone di lino con cuoio	XIV sec	16,5x10,5	20,9	51,2	30,3	144,98	16,5x10,5	19,7
14	Spartito musicale	XIII sec	6,5x15,8	1,86	4,1	2,24	120,43	6,5x15,8	1,7

Tabella 1. Dati relativi ai campioni utilizzati per il test di liofilizzazione eseguito presso il Politecnico di Torino.

Si è cercato di mantenere fin dalla preparazione dei campioni uno spessore ridotto, in quanto i tempi del processo di sublimazione sono direttamente proporzionali a questa misura.



Figura 2. I campioni bagnati sono stati leggermente strizzati e lasciati a sgocciolare l'acqua in eccesso.

Un ulteriore dato positivo emerso da questo esperimento è stato che i campioni di carta patinata una volta trattati, mantengono inalterate le loro proprietà anche se sottoposti a successiva ribagnatura.



Figura 3. Pesatura dei campioni a processo ultimato.



Figura 4. Le modificazioni macroscopiche dei beni a processo ultimato sono state registrate e catalogate.

L'esperimento condotto ha consentito di verificare che il processo di liofilizzazione non abbia compromesso in maniera definitiva nessuno dei campioni sottoposti a trattamento. Alcune deformazioni visibili a processo ultimato non sono si sono mantenute nel tempo, mentre per altre, come ad esempio l'imbarcatura delle copertine rigide in cartoncino rivestito di cuoio (fig. 4) è sufficiente prevedere di posizionare dei pesi già nel liofilizzatore per stabilizzare le superfici.

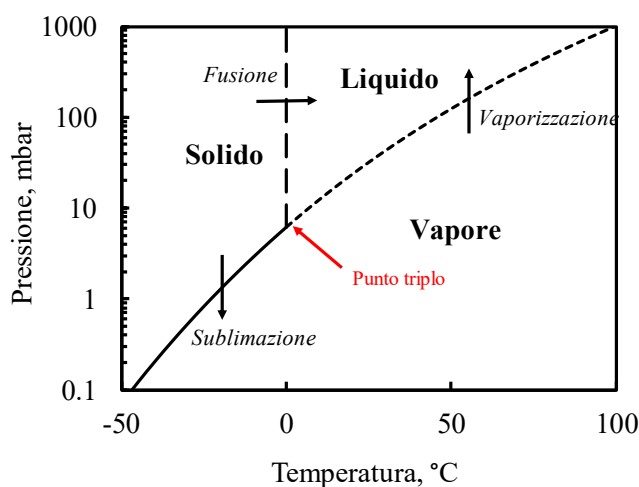
Liofilizzazione di materiale cartaceo (a cura di Davide Fissore e Antonello Barresi, DISAT, Politecnico di Torino, Laboratorio di Liofilizzazione)

Definizione e concetti generali

La liofilizzazione è un processo di essiccamento nel quale un liquido, in genere acqua, preventivamente congelato, viene rimosso da un prodotto mediante sublimazione.

La sublimazione del ghiaccio, ovvero il suo passaggio diretto dallo stato solido allo stato di vapore, senza passare dallo stato liquido, ha luogo dipendentemente dalle condizioni di temperatura e pressione in cui si trova il materiale.

La figura seguente presenta il digramma di stato dell'acqua ed evidenzia gli intervalli di temperatura e di pressione in cui l'acqua si presenta nelle varie forme (solido, liquido, vapore), mostrando come al di sotto del punto triplo, ovvero ad una pressione inferiore a 6.11 mbar, all'aumentare della temperatura l'acqua non possa che passare dallo stato solido a quello vapore.



Il fatto che la rimozione dell'acqua avvenga senza il passaggio attraverso la fase liquida consente di ottenere un prodotto di elevata qualità, nel quale le caratteristiche qualitative, come struttura e aspetto, del prodotto iniziale vengono preservate. Nel caso di materiali bagnati l'essiccamento per liofilizzazione consente di evitare fenomeni di arricciamento e accartocciamento, mantiene il colore originario, etc.

Fasi del processo

Preliminare al processo di liofilizzazione è il congelamento del prodotto, dove l'abbassamento di temperatura consente il passaggio dell'acqua dallo stato liquido a quello solido. A tal proposito è da

rilevare che non tutta l'acqua congela, ma solamente la cosiddetta acqua "libera", ovvero quella non legata alle molecole (proteine, carboidrati, ...) del prodotto solido, mentre una certa frazione di acqua, l'acqua "legata", non diviene ghiaccio, e rimane legata alle molecole del materiale. La frazione di acqua "legata" è dipendente dalle caratteristiche del prodotto, e in genere non supera qualche percento del totale.

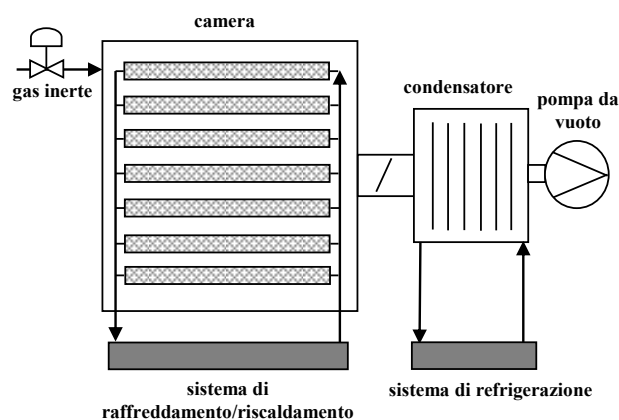
La liofilizzazione prevede due fasi consecutive: l'essiccamento primario, nella quale il ghiaccio sublima, consentendo così la completa rimozione dell'acqua libera, e l'essiccamento secondario, nella quale si riduce il contenuto di acqua legata facendola desorbire dal prodotto (occorre rilevare comunque che anche durante l'essiccamento primario ha luogo il desorbimento dell'acqua nella porzione di prodotto essiccato).

Le condizioni operative (temperatura e pressione) delle due fasi sono differenti: in genere l'essiccamento secondario viene condotto ad una temperatura superiore rispetto a quella dell'essiccamento primario al fine di agevolare il processo di desorbimento dell'acqua legata.

Nel caso in cui ad essere liofilizzati siano libri e materiale cartaceo si può comunque ritenere soddisfacente la deumidificazione che si ottiene al termine dell'essiccamento primario, dal momento che non è di interesse disidratare completamente il prodotto.

Occorre sottolineare che la sublimazione del ghiaccio è un processo endotermico, così come il desorbimento dell'acqua legata, e, quindi, è necessario fornire energia al prodotto durante l'intero processo. In particolare, il calore di sublimazione del ghiaccio è pari a 2836 kJ/kg (a 0°C).

La figura seguente presenta uno schema di massima di una apparecchiatura dove condurre il processo di liofilizzazione.



Il prodotto viene caricato in una camera che presenta dei ripiani all'interno dei quali viene fatto scorrere un fluido che fornisce calore al prodotto durante la liofilizzazione. Il prodotto può essere riscaldato anche

con altre modalità, ad esempio mediante riscaldatori elettrici.

La fase di congelamento può essere condotta separatamente, in altra apparecchiatura, o all'interno della camera di liofilizzazione e, in questo caso, è necessario usare ripiani con circolazione di fluido a temperatura molto bassa, così da determinare il raffreddamento e il congelamento dell'acqua.

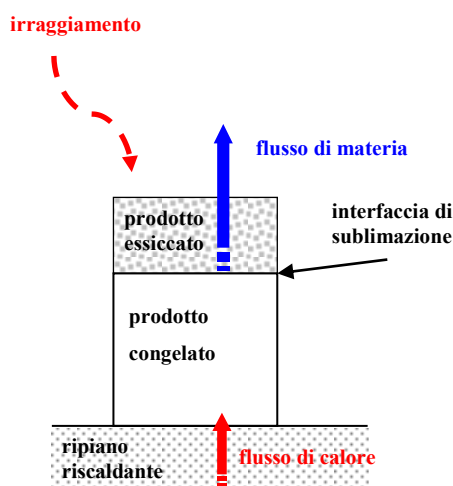
Una pompa da vuoto viene utilizzata per abbassare la pressione all'interno della camera di liofilizzazione, avviando così la fase di sublimazione.

Tra la camera e la pompa viene posto un condensatore, dove viene fatto brinare il vapore d'acqua (con un opportuno sistema di refrigerazione), così da ridurre la portata volumetrica di gas che la pompa da vuoto deve evacuare.

Talvolta viene introdotta nella camera di liofilizzazione una corrente di gas inerte (azoto), per assicurare un più accurato controllo della pressione nella camera stessa.

Nella fase di essiccamento primario si osserva la formazione di una interfaccia mobile di sublimazione che separa il prodotto congelato, nella parte inferiore, dal prodotto essiccato, nella parte superiore. Il vapore si allontana dal prodotto muovendo dall'interfaccia di sublimazione verso la camera, attraversando quindi il prodotto essiccato, e causando lo spostamento dell'interfaccia che si muove verso il basso man mano che il processo va avanti.

Il prodotto riceve l'energia necessaria alla sublimazione dal ripiano riscaldante e, talvolta, anche per irraggiamento dalle pareti della camera di liofilizzazione.



Scelta delle condizioni operative e durata del processo.

Le condizioni operative del processo, ovvero la temperatura del ripiano riscaldante e la pressione nella

camera di liofilizzazione, devono essere accuratamente scelte in modo tale da evitare di danneggiare il prodotto e di prolungare eccessivamente la durata del processo, che può raggiungere anche parecchi giorni.

Il flusso di sublimazione è descrivibile mediante la seguente espressione:

$$J_w = \frac{1}{R_p} (p_{w,i} - p_{w,c})$$

dove J_w è il flusso di sublimazione dell'acqua ($\text{kg s}^{-1}\text{m}^{-2}$), $p_{w,i}$ (Pa) è la tensione di vapore del ghiaccio, $p_{w,c}$ (Pa) è la pressione parziale del vapore nella camera di liofilizzazione, e R_p (m s^{-1}) è la cosiddetta resistenza dello strato secco al flusso di vapore.

In genere $p_{w,c}$ viene assunto pari al valore della pressione in camera di liofilizzazione, dal momento che l'atmosfera in camera è composta prevalentemente da acqua. Il termine $p_{w,i}$ è invece funzione (nota) della temperatura dell'interfaccia di sublimazione e, in particolare, aumenta all'aumentare di tale temperatura (varia da 0.38 mbar a -30°C , a 1.03 mbar a -20°C , a 2.6 mbar a -10°C a 6.1 mbar a 0°C).

Il termine R_p è una caratteristica del prodotto processato, ed aumenta all'aumentare dello spessore del prodotto stesso.

A parità di tutto, all'aumentare dello spessore aumenta quindi la resistenza del prodotto essiccato al flusso di vapore e, quindi, diminuisce il flusso di sublimazione con un corrispondente aumento della durata del processo.

Risulta quindi di fondamentale importanza controllare lo spessore del prodotto inserito nella camera di liofilizzazione, che non dovrebbe essere superiore a qualche cm.

L'esame dell'espressione precedente evidenzia come sia quindi maggiormente interessante lavorare a pressione decisamente inferiore a quella del punto triplo, poiché questo determina un aumento della velocità di sublimazione, soprattutto quando è particolarmente importante la resistenza offerta dal materiale al flusso di vapore, vuoi per lo spessore dello stesso, vuoi per la natura della matrice. Il flusso di sublimazione aumenta inoltre all'aumentare della temperatura del prodotto.

La scelta delle condizioni operative cui condurre il processo di liofilizzazione dovrebbe quindi essere lasciata a personale qualificato ed esperto nel settore, così da garantire il raggiungimento delle caratteristiche desiderate nel prodotto finale, nonché una durata del processo non eccessivamente elevata.

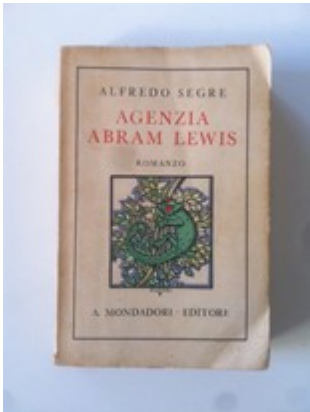
La durata del processo è una funzione complessa di molti parametri, ed è funzione non lineare dello spessore del materiale che si sta essiccando. Ciò vuol dire che se, ad esempio, per liofilizzare un

materiale avente spessore pari a 1 cm sono necessarie 10 ore, per liofilizzare un materiale avente le medesime caratteristiche, ma uno spessore di 2 cm è necessario un tempo che può essere significativamente superiore alle 20 ore. Se possibile, non ha quindi interesse caricare sui ripiani del liofilizzatore materiale di spessore eccessivo. Inoltre, sarebbe opportuno disporre sul liofilizzatore materiale di spessore uniforme, così da utilizzare l'apparecchiatura nel modo più efficiente possibile.

Per comprendere l'evoluzione del prodotto durante il processo di liofilizzazione si consideri il seguente caso di studio, ovvero la liofilizzazione di un volume di dimensioni pari a 12x19.2x2.7 (cm) e peso pari a 350.6 g.

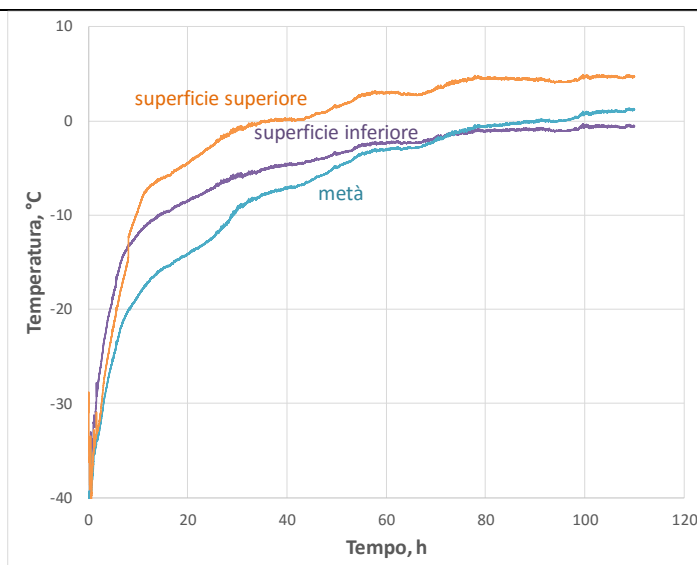
Il volume è stato inizialmente immerso in una bacinella contenente acqua per un tempo pari a 6 h. A valle di ciò il peso del volume è risultato essere pari a 755 g, ovvero la variazione di peso è stata pari al 115% circa.

La liofilizzazione è stata condotta a 0.1 mbar e disponendo il prodotto su un ripiano riscaldato a 10°C, ed al termine del processo il volume è risultato avere dimensioni pari a 12x19.2x3.0 (cm) e peso pari a 352 g.

<i>Volume originale</i>	<i>Volume bagnato inserito nel liofilizzatore</i>	<i>Volume al termine del processo di liofilizzazione</i>
		

Per studiare l'evoluzione del prodotto durante il processo sono state inserite nel volume tre termocoppie, una in corrispondenza della superficie superiore, poche pagine al di sotto della copertina, una in corrispondenza della superficie inferiore, poche pagine al di sopra della copertina, ed una a metà circa del volume.

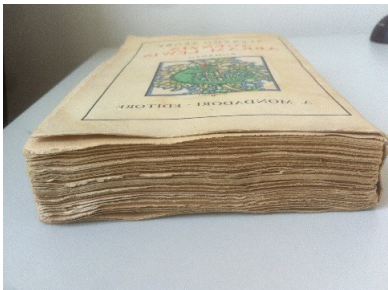
La figura seguente mostra l'evoluzione della temperatura misurata dalle termocoppie.



Osservando l'andamento della temperatura in corrispondenza della superficie inferiore e della metà del volume si osserva come la temperatura di quest'ultima sia inferiore rispetto alla superficie inferiore come è logico attendersi, dal momento che il calore arriva nel prodotto dal basso. Si osserva però anche come la temperatura in corrispondenza della superficie superiore sia più elevata delle altre, e questo per effetti di irraggiamento dalle pareti della camera di liofilizzazione. Il contributo dell'irraggiamento spiega anche perché la temperatura misurata sia superiore, di qualche grado, alla temperatura del ripiano riscaldante.

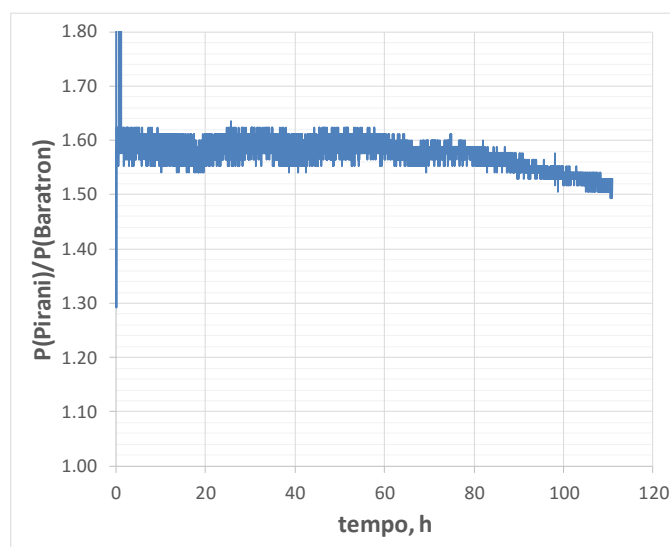
L'andamento delle temperature è abbastanza significativo, con un tratto iniziale crescente, e una sorta di andamento asintotico da un certo momento in avanti, soprattutto per le temperature misurate alle estremità superiore ed inferiore del volume, con un valore che dovrebbe essere pari a quello del fluido riscaldante, o di qualche grado superiore qualora l'irraggiamento influenzi la dinamica del sistema. Quando viene raggiunto questo asintoto orizzontale significa che l'essiccamento primario in quella porzione del volume è completato, e la temperatura non varia più. Con le condizioni operative adottate risulta che dopo circa 3 giorni l'essiccamento è completato alle due estremità del volume, mentre nella parte centrale è ancora presente del ghiaccio..

Il processo è stato interrotto dopo 110 ore dall'inizio, e ci si attende quindi la presenza di una piccola quantità di ghiaccio nella parte centrale del volume. Questa è stata osservata a valle del processo: poche ore dopo l'allontanamento del volume dalla camera di liofilizzazione, la piccola quantità di ghiaccio si è sciolta, come mostrato nella figura seguente. Dopo pochi giorni a temperatura ambiente, la rapida diffusione di questa piccola quantità di acqua ha consentito di riportare il volume nelle condizioni iniziali.

<i>Volume al termine della liofilizzazione</i>	<i>Tracce di umidità nella parte centrale</i>	<i>Aspetto della parte centrale del volume dopo pochi giorni</i>
		

Che la liofilizzazione nel campione non fosse completata lo si poteva dedurre anche dall'osservazione dell'andamento nel tempo della curva del rapporto tra le pressioni misurate in camera da un sensore di pressione di tipo termocoduttivo (tipo Pirani) e di tipo capacitivo (tipo Baratron). Tali sensori di pressione sono normalmente disponibili in una apparecchiatura per la liofilizzazione.

Tale curva ha in un processo di liofilizzazione un andamento caratteristico, con un andamento orizzontale nel tempo per la maggior parte della fase di essiccamento primario, per poi scendere verso un asintoto orizzontale quanto l'essiccamento va a essere concluso. In questo caso l'essiccamento è stato terminato quando la curva aveva ancora un andamento debolmente decrescente, e non si era raggiunto il secondo asintoto, e pertanto l'essiccamento non poteva dirsi concluso.



Occorre però evidenziare che l'aver interrotto il processo dopo 110 h dal suo inizio non ha compromesso le caratteristiche del prodotto finale: la quantità di ghiaccio residua nel prodotto non è stata infatti tale da compromettere le caratteristiche del prodotto al termine della liofilizzazione.

Anche in questo caso è necessario che la durata del processo di liofilizzazione venga determinata da personale qualificato ed esperto, che valuti il momento ottimale cui interromperlo, evitando così di prolungarlo senza che ve ne sia una reale necessità.

Osservazioni conclusive

Quanto illustrato in precedenza consente di formulare dei suggerimenti per la gestione di alcuni aspetti dell'archiviazione di materiale cartaceo e archivistico, e della gestione di alcuni aspetti della fase di emergenza. In particolare:

1. E' opportuno, a valle dell'allagamento, procedere al congelamento del materiale il prima possibile, così da ridurre il tempo in cui l'acqua liquida è a contatto col materiale;
2. Il materiale da destinarsi al congelamento, se possibile, ha da essere raggruppato in modo tale da non avere blocchi di spessore eccessivo (l'obiettivo potrebbe essere uno spessore di 1-2 cm). Ciò consente sia di velocizzare la fase di congelamento, minimizzando i potenziali danni derivanti dal contatto dell'acqua liquida col supporto cartaceo, nonché di velocizzare la fase di essiccamento (liofilizzazione). Va da sé che se non è possibile suddividere il materiale da congelare in blocchi di ridotto spessore, sarà necessario procedere alla liofilizzazione del materiale così come è.
Si suggerisce, in questo caso, di modificare le modalità di archiviazione, soprattutto nel caso di faldoni, così da avere il materiale archiviato in faldoni di spessore ridotto, cosa che, come detto, favorirebbe la fase di gestione delle emergenze.
3. Il processo di liofilizzazione ha da essere condotto a condizioni di temperatura e pressione opportune, così da minimizzarne la durata, consentendo il ripristino del materiale nel tempo minore possibile (e quindi con costi inferiori, soprattutto quelli di stoccaggio del materiale congelato).
4. Il processo di liofilizzazione va condotto sino al completo allontanamento del ghiaccio. In caso contrario il materiale è in parte completamente essiccato, ed in parte contiene la medesima quantità di acqua che presenta ad allagamento avvenuto, con le ovvie conseguenze.
5. A valle del processo di liofilizzazione, dipendentemente dalle caratteristiche del materiale trattato, può essere necessario immagazzinare il materiale in un ambiente a umidità controllata per ripristinare il corretto quantitativo di umidità nel materiale. La liofilizzazione consente infatti di preservare le caratteristiche qualitative del materiale, ma porta al completo allontanamento dell'acqua presente.
6. La liofilizzazione non può risolvere le problematiche dovute al contatto del materiale con l'acqua

liquida: si tratta di un processo che consente di deumidificare un materiale preservandone (il più possibile) le caratteristiche qualitative, rendendo nuovamente il materiale cartaceo/archivistico fruibile all'utenza, ma i danni irreversibili avvenuti col contatto con l'acqua liquida non possono essere corretti (per questa ragione occorre procedere al congelamento del materiale il prima possibile).

PIANO DELLA FORMAZIONE

L'efficacia del Piano si misura in base alla diffusione dei suoi contenuti e concertazione delle sue prescrizioni operative.

Al fine di rendere prassi le buone pratiche proposte e formare adeguatamente il personale a disposizione ad eseguire correttamente le operazioni previste, è necessario programmare nel tempo una serie di incontri teorici, di aggiornamento e pratici.

Giornate di formazione

In questa dicitura si considerano anche i momenti di concertazione tra personale tecnico che progetta il piano, l'ente gestore e il personale che sarà effettivamente incaricato di eseguirlo (personale dell'archivio, protezione civile locale, comando dei vigili del fuoco, volontari autorizzati, autorità locali,...).

Specificare data, attività previste, numero e nome dei partecipanti, risultati e punti di discussione.

Programmazione delle giornate successive.

Esercitazioni

Data, attività previste, numero e nome dei partecipanti.

Descrizione e report finale dell'attività.

Programmazione delle esercitazioni successive.

Note

Segnalazione di possibili criticità emerse, necessità di rivedere modello e metodologia.

PIANO DI MONITORAGGIO E REVISIONE

In questa sezione si richiede di monitorare e registrare l'efficacia del PIANO DI CONOSCENZA PER LA SICUREZZA DI ARCHIVI E BIBLIOTECHE, di rivedere e aggiornarne i contenuti in riferimento a successivi eventi o nuove tecniche o risorse a disposizione.

Valutazione dell'efficacia del Piano nel tempo, registrazione dell'implementazione e degli impatti del piano nel medio e lungo periodo.

Definire KPI (Key Performance Indicator) caratterizzanti.

Riportare lo stato di avanzamento della realizzazione del piano.

Queste indicazioni sono finalizzate a stabilire le modalità e i contenuti delle revisioni periodiche del Piano complessivo.

OBIETTIVO STRATEGICO	INDICATORE	VALORE		
		anno	anno	anno
Conoscenza dell'archivio	Numero di sopralluoghi effettuati			
	Numero di indagini eseguite			
	...			
Messa in sicurezza dei locali	Numero delle contromisure gestionali adottate			
	Numero delle contromisure strutturali adottate			
	...			
Messa in sicurezza del materiale	Numero di elementi danneggiati in un anno			
	Numero delle contromisure gestionali adottate			
	Numero di interventi di restauro/recupero richiesti			
	Attività di scarto			
	...			
Formazione	Numero di giornate di formazione			
	Numero di partecipanti			

SOPRINTENDENZA ARCHIVISTICA e BIBLIOGRAFICA DELLA LOMBARDIA*Piano di Conoscenza per la Sicurezza di Archivi e Biblioteche**A cura di Paola Mussini, Luciano Sassi – giugno 2016*

	Numero di partecipazione ad eventi di formazione esterni			
	Numero di esercitazioni condotte			
Gestione delle risorse	Risorse economiche allocate per l'incremento della sicurezza dei locali			
	Risorse economiche allocate per materiali utili durante le emergenze			
...				

ALLEGATO 1 - SCHEDA RILEVAZIONE DANNI

Eseguire una dettagliata attività di schedatura in situazioni di emergenza, potrebbe risultare poco agevole (richiede tempo e risorse che spesso mancano) e di fatto anche poco utile e dispersivo.

E' comunque importante considerare che una documentazione completa dello stato dell'evento e delle sue conseguenze immediate siano estremamente utili in fase di gestione delle pratiche assicurative o di contenziosi per danni derivati da cause derivate da azioni errate da parte di imprese di manutenzione, errori di costruzione, ecc...

In concordanza con quanto introdotto in **Premessa**, deve controllare la resistenza dei dati identificativi di ogni bene, eventualmente aggiungendo in fase preventiva un codice identificativo su ogni bene, a matita, in modo tale quindi da essere leggibile anche se bagnato e facilmente rimuovibile.

Nel caso invece in cui la situazione specifica permetta anche di eseguire questa operazione senza impattare sul salvataggio emergenziale dei beni coinvolti, è possibile fare riferimento alla scheda elaborata da *MiBACT – Direzione Generale Archivi, Linee guida per la prevenzione dei rischi e la reazione alle emergenze negli archivi*.

Proponiamo di seguito una bozza di scheda speditiva di primo sopralluogo post evento, redatta dalla Soprintendenza Archivistica per la Lombardia al fine di registrare dati relativi agli archivi colpiti dal sisma del 2009 nel mantovano.

Informazioni scheda

Riferimento a eventuale scheda edificio:

Riferimento a evento calamitoso e data:

Numero scheda di rilevazione dati:

Provincia:

Comune:

Data rilevazione:

Referente tecnico Soprintendenza Archivistica

Nome e cognome:

Qualifica:

Recapito telefonico: Mail:
<i>Responsabili possesso e detenzione del bene</i>
Ente: Nome e Cognome: Recapito telefonico: Mail:
<i>Complesso archivistico- biblioteca</i>
Archivio storico, di deposito, biblioteca, ecc...
<i>Collocazione dell'archivio - biblioteca</i>
Indirizzo dell'edificio.
<i>Consistenza della documentazione</i>
N. unità archivistiche - librerie: Metri lineari:
<i>Strumenti descrittivi</i>
Inventari: Elenchi di consistenza: Altro:
<i>Situazione della sede</i>
Riportare informazioni riguardanti: • il grado di accessibilità dell'immobile • le condizioni strutturali • le condizioni impiantistiche • le condizioni delle scaffalature
<i>Interventi necessari</i>
• si richiede un pronto intervento in emergenza

- non è necessario un pronto intervento in emergenza

Indicazioni per il restauro e la conservazione

Indicazioni per la corretta esecuzione delle future operazioni di restauro e conservazione del bene, alla luce delle possibili vulnerabilità acquisite.

Localizzazione

Indicazioni localizzative del bene a seguito dell'evento (ricovero di emergenza, ...)

Rilievo fotografico

Rilievo fotografico del bene danneggiato, le immagini vanno opportunamente nominate in modo da poter essere facilmente identificate nel testo.

Se possibile riportare delle immagini riferibili alle condizioni pre-danno del bene.

Datazione della campagna di rilievo.

ALLEGATO 2a - SCHEDA PRONTO INTERVENTO

La registrazione delle attività svolte costituisce parte della documentazione utilizzata per l'istruttoria assicurativa, pertanto si consiglia di tracciare scrupolosamente quanto eseguito.

Compilatore

Nome e contatti del compilatore della scheda e del personale che esegue l'attività di pronto intervento.

Data

Data in cui è stato eseguito l'intervento e data di compilazione

Motivazione dell'intervento

Descrizione dell'evento che ha determinato il danno.

Riferimento a documenti specifici sull'evento.

Valutazione delle modalità di impatto.

Codice evento e numero progressivo intervento

Numero identificativo della scheda creato da tipologia evento, data, numero progressivo della scheda,...

Riferimento codice della scheda di danno.

Descrizione dell'intervento

Descrizione sommaria dell'oggetto archivistico in esame e del danno subito, nonché del tipo di intervento eseguito, descrizione delle varie fasi, motivazione delle scelte e rilevazione delle criticità.

Operatore

Indicare l'operatore che ha eseguito l'intervento se diverso dal compilatore

Indicazioni per il restauro e la conservazione

Indicazioni per la corretta esecuzione delle future operazioni di restauro e conservazione del bene, alla luce delle possibili vulnerabilità acquisite.

Rilievo fotografico

Le immagini vanno opportunamente nominate in modo da poter essere facilmente identificate nel

testo, le diverse fasi vanno documentate.

Se possibile riportare delle immagini riferibili alle condizioni pre-danno del bene. *Questo dato è importante perché testimonia lo stato ante facto e andrebbe rilevato in fase di raccolta dati per la compilazione del piano, chiaramente non per tutti i beni contenuti, ma magari per quelli più importanti, così dei depositi e dei luoghi occupati dall'istituto.*

Datazione della campagna di rilievo.

ALLEGATO 2b - REPORT INTERVENTO

Stilare una descrizione complessiva dell'intervento eseguito a seguito del verificarsi di un evento, con riferimento a tutte le schede di danno e di intervento in emergenza compilate. Questo report ha anche lo scopo di ricordare ed ordinare tutte le operazioni avvenute, con le decisioni avvenute e la motivazione, l'eventuale discordanza con il PRE a causa di forza maggiore – da indicare. La documentazione fotografica e la precisione del report nonché la citazione delle persone/personale coinvolte da un valore probante alle procedure intraprese in fase di contenzioso.

ALLEGATO 3 – ETICHETTA CASSE

Istituto _____

Luogo di destinazione _____

Numero della cassa _____

Data _____

DOCUMENTI ASCIUTTI

Istituto _____

Luogo di destinazione _____

Numero della cassa _____

Data _____

DOCUMENTI UMIDI

Istituto _____

Luogo di destinazione _____

Numero della cassa _____

Data _____

DOCUMENTI BAGNATI

RIFERIMENTI

VALUTAZIONE DEL RISCHIO

BROKERHOF A., MEUL V., MICHALSKI S., PEDERSOLI J.L., *Advancing Research in Risk Management Applications to Cultural Property*, ICCROM Newsletter 33, Roma, June 2007, pp. 10-11.

D.lgs. 9 aprile 2008 n. 81 e s.m., *Testo Unico sulla Salute e Sicurezza sul Lavoro*.

D.P.R. 1 agosto 2011 n. 151, *Schema di regolamento per la disciplina dei procedimenti relativi alla prevenzione incendi*. <http://www.vigilfuoco.it/aspx/page.aspx?IdPage=5574>

HER MAJESTY TREASURY, *The Orange Book. Management of Risk – Principles and Concepts*, London 2004. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

ICR – ISTITUTO CENTRALE DEL RESTAURO, *Carta del rischio dei beni culturali*. <http://www.cartadelrischio.it/ita/ambientearia.asp>

ISO 31000:2009, *Risk management – Principles and guidelines*.

ISO 11799:2003, *Information and documentation — Document storage requirements for archive and library materials*.

ISO Guide 73:2009, *Risk management – Vocabulary*.

ISO/IEC 31010:2009, *Risk management – Risk assessment techniques*.

MATTHEWS G., SMITH Y., KNOWLES G., *Disaster Management in Archives, Libraries and Museums*, Ashgate Publishing Limited, 2009 (Cap. 2).

MIBAC, Circolare n. 26/2010, *Linee guida per la valutazione e riduzione del rischio sismico del patrimonio culturale allineate alle nuove Norme tecniche per le costruzioni*, 2010.

OHSAS 18001 - *Health & Safety standard*.

SHANG K., HOSSEN Z., *Applying Fuzzy Logic to Risk Assessment and Decision-Making*, *Casualty Actuarial Society*, Canadian Institute of Actuaries, Society of Actuaries, 2013. <https://web.actuaries.ie/sites/default/files/erm-resources/research-2013-fuzzy-logic.pdf>

STOVEL H., *Risk Preparedness: a management manual for world cultural heritage*, ICCROM, Roma 1998 (Cap. 2/4 per concetti generali, Cap. 5/9 per descrizione pericoli). http://www.iccrom.org/ifrcdn/pdf/ICCROM_17_RiskPreparedness_en.pdf

UNESCO, *Managing disaster risks for World Heritage*, Parigi 2010 (Cap. 1/3). <http://whc.unesco.org/en/managing-disaster-risks/>

UNISDR, *Terminology on disaster risk reduction*, 2009. <http://www.unisdr.org/we/inform/publications/7817>

WALLER R., MICHALSKI S., *Effective preservation: from reaction to prediction*, in *Conservation: the Getty Conservation Institute newsletter*, Vol. 19, N. 1, 2004, p. 4-9. http://www.getty.edu/conservation/publications/newsletters/19_1/feature.html

PROCEDURE E INTERVENTI

AUSTRALIAN GOVERNMENT AND NATIONAL ARCHIVES OF AUSTRALIA, *National Disaster Preparedness and recovery Strategy for Archival Records*, 2010. http://www.naa.gov.au/Images/ndprs_tcm16-49144.pdf

BERTINI M.B., *La conservazione dei beni archivistici e librari. Prevenzione e piani di emergenza*, Carocci Editore, Roma 2005.

BERTINI M.B., *Linee guida per una conservazione preventiva responsabile*, in Petrilli Vincenza (a cura di), *I custodi della memoria. L'edilizia archivistica italiana statale del XX secolo*, Maggioli Editore, Santarcangelo di Romagna 2014, pp. 111-140.

BIASOTTI A., *Il piano di emergenza per i beni culturali*, Tipografia A.T. I., Pomezia, 2006.

DADSON E., *Emergency Planning and Response For Libraries, Archives and Museums*, Facet, London 2012.

IFLA/AIB, *Principi dell'IFLA per la cura e il trattamento dei materiali di biblioteca*, AIB, Roma 2005. <http://www.aib.it/negozio-aib/pubblicazioni/principi-dellifla-per-la-cura-e-il-trattamento-dei-materiali-di-biblioteca/>

MATTHEWS G., SMITH Y., KNOWLES G., *Disaster Management in Archives, Libraries and Museums*, Ashgate Publishing Limited, 2009 (Cap. 5).

MIBAC, Circolare n. 132 8 ottobre 2004, *Piani di emergenza per la tutela del patrimonio culturale*. http://www.beniculturali.it/mibac/export/SG-MiBAC/sito-SG-MiBAC/Contenuti/Temi/Sicurezza/visualizza_asset.html_1691482669.html

MIBAC, Circolare n.30 6 febbraio 2007, *Piani di emergenza per la tutela del patrimonio culturale – pianificazione e gestione delle esercitazioni*. http://www.beniculturali.it/mibac/export/SG-MiBAC/sito-SG-MiBAC/Contenuti/Temi/Sicurezza/visualizza_asset.html_350654039.html

MIBACT, Direttiva 12 dicembre 2013, *Procedure per la gestione delle attività di messa in sicurezza e salvaguardia del patrimonio culturale in caso di emergenze derivanti da calamità naturali*. http://www.beniculturali.it/mibac/multimedia/MiBAC/documents/1396342272741_Direttiva_12_12_2013.pdf

MIBACT – Direzione Generale Archivi, *Linee guida per la prevenzione dei rischi e la reazione alle emergenze negli archivi*, 2014 <http://www.archivi.beniculturali.it/index.php/cosa-facciamo/progetti-di-tutela/gruppi-di-studio/item/95-gruppi-di-studio-%7C-emergenze>

MIBACT, Direttiva 23 aprile 2015, *Aggiornamento della direttiva 12 dicembre 2013, relativa alle Procedure per la gestione delle attività di messa in sicurezza e salvaguardia del patrimonio culturale in caso di emergenze derivanti da calamità naturali*. http://www.beniculturali.it/mibac/multimedia/MiBAC/documents/1437986288170_DIRETTIVA_23Aprile2015.pdf

MIBACT, Circolare n. 15, 30 aprile 2015, *Disposizioni in materia di tutela del patrimonio architettonico e mitigazione del rischio sismico*.

ORMANNI E., *L'organizzazione di un servizio di pronto intervento*, Bollettino dell'Istituto centrale per la patologia del libro "Alfonso Gallo", v. 36., 1980, speciale, 365-375.

http://www.icpal.beniculturali.it/scheda_periodico.html?ids_foto=1240B69B-A686-4694-8AA2-E7B11B67AB0D

PROSPERI C., *L'alluvione e gli archivi*, CAB newsletter : conservazione negli archivi e nelle biblioteche, v. 4., 1995, 16, 3-4 http://www.icpal.beniculturali.it/scheda_periodico.html?ids_foto=66E5D665-CEB6-45F7-B2AD-EBC1306103E6

PROVINCIA AUTONOMA DI TRENTO, Deliberazione n. 1759 12 ottobre 2015, *Linee guida per la protezione*

del patrimonio archivistico e librario trentino. <https://www.cultura.trentino.it/Il-Dipartimento/Soprintendenza-per-i-beni-culturali/Ufficio-beni-archivistici-librari-e-Archivio-provinciale/Strumenti/1-Linee-guida-per-la-protezione-del-patrimonio-archivistico-e-librario-trentino>

REGIONE LOMBARDIA – DIREZIONE GENERALE CULTURE, IDENTITÀ E AUTONOMIE DELLA LOMBARDIA, *Beni librari e documentari. raccomandazioni per la tutela*, Milano, 2007.

SOPRINTENDENZA ARCHIVISTICA PER IL PIEMONTE E LA VALLE D'AOSTA, *Sedi d'archivio: caratteristiche e requisiti*, http://www.sato-archivi.it/Sito/images/stories/modelli_scaricabili/requisiti_strutturali_archivio.pdf

SKEPASTIANU M., WHIFFIN J. I., *Piano per la prevenzione dei disastri in biblioteca : prevenzione, pronto intervento, reazioni, recupero*, CAB newsletter : conservazione negli archivi e nelle biblioteche. Nuova serie, v. 1., 1996, 2, 3-7. http://www.icpal.beniculturali.it/scheda_periodico.html?ids_foto=AB7BF66E-C864-474D-8208-D2479D410AD2

STOVEL H., *Risk Preparedness: a management manual for world cultural heritage*, ICCROM, Roma 1998 (Cap. 10). http://www.iccrom.org/ifrcdn/pdf/ICCROM_17_RiskPreparedness_en.pdf

UNESCO, *Managing disaster risks for World Heritage*, Parigi 2010 (Cap. 4/6, 8) <http://whc.unesco.org/en/managing-disaster-risks/>

LIOFILIZZAZIONE

BARRESI A., CAPOLONGO A., ROVERO G., *Soaking and freeze-drying of paper simulating water damaged documets for salvage of archival materials*, European Congress of Chemical Engineering, Granada 2003.

BARRESI A., CAPOLONGO A., *Freeze-drying of water-damaged paper material*, Restaurator 119-128, 2004.

BICCHIERI M., MONTI M., FRATI & LIVI S.R.L., *La liofilizzazione quale intervento di recupero di volumi danneggiati da catastrofi naturali*, AIAR Pisa 2006.

CARAPELLE A., HENRIST M., RABECKI F., *A study of vacuum freeze-drying of frozen wet papers*, Drying Technology: An International Journal, vol. 19, Issue 6, 2001.

CARLSEN S., *Effects of freeze drying on paper*, IADA Conference 1999.

CRESPI E., CAPOLONGO A., FISSORE D., BARRESI A., *Experimental Investigation of the Recovery of Soaked paper Using Evaporative Freeze Drying*, Drying Technology 26: 349-356, 2008.

GUASTI G., SIDOTI A. (a cura di), *Biblioteca Nazionale Centrale di Firenze. Piano di Emergenza per il salvataggio delle collezioni*, III aggiornamento 2014.

GUPTA H., CHATTERJEE S. G., *Parallel Diffusion of Moisture in Paper Part 1: Steady-State Conditions*, Industrial & Engineering Chemistry Research, vol. 42, no. 25, 2003.

MCLEARY J. P., *Vacuum freeze-drying, a method used to salvage water-damaged archival and library materials: a RAMP study with guidelines prepared for the General Information Programme and UNISIST*, UNESCO Paris, 1987.

RAMRAO B. V., MASSOQUETE A., LAVRYKOV S., RAMASWAMY S., *Moisture Diffusion Inside Paper Materials in the Hygroscopic Range and Characteristics of Diffusivity Parameters*, Drying Technology vol. 21, no. 10, pp. 2007-2056, 2003.

SUGARMAN J. E., VITALE T. J., *Observations an the drying of paper: five drying methods and the drying*

process, Journal of the American Institute for Conservation, vol. 31, number 2, article 3, pp. 175-197, 1992.

THOMAS D., FLINK J.M., *Microwave drying of water soaked books*, Journal of Microwave Power 9 (4): 349-354, 1974.

TREMAIN D., *Notes on Emergency Drying of Coated Papers damaged by Water*, <http://cool.conservation.org/byauth/tremain/coated.html>

WALSH B., *Salvage operations for water managed archival collections: a second glance*, Canadian Council of Archives, 2003.

WATERS P., *Procedures for Salvage of water damaged library materials*, 2016.

1. Composizione del piano

Il Piano di Conservazione dell'archivio, oltre che dai seguenti articoli, è composto dal Titolare di Classificazione e il Massimario di scarto di Regione Lombardia (All. 1).

2. Titolare di classificazione

È adottato il Titolare di Classificazione e Massimario di Scarto della documentazione del sistema Sanitario e Socio Sanitario di Regione Lombardia vigente di cui all'Allegato 1; il suo aggiornamento compete alla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi. La funzione del Titolare di classificazione è collegata al concetto di archiviazione dei documenti protocollati: l'esatta attribuzione di una classificazione ad un documento consente di individuare la sua collocazione logica all'interno dell'archivio sia analogico sia informatico. Il Titolare è costituito da tre titoli cui corrispondono le tre aree costitutive delle aziende sanitarie: area amministrativa (Titolo 1), area sanitaria e socio-sanitaria territoriale (Titolo 2), area ospedaliera (Titolo 3). La classificazione del documento si riferisce quindi al contenuto dell'atto e non necessariamente all'ufficio dell'Agenzia che lo ha prodotto.

Il sistema informatico adottato dall'Agenzia garantisce la storicizzazione delle variazioni del Titolare e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti in relazione al Titolare vigente al momento della produzione degli stessi.

Per ogni modifica del Titolare, deve essere riportata la data di introduzione o quella di variazione, cioè la durata della stessa.

Ad ogni modifica, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e ad impartire le istruzioni per il corretto utilizzo delle nuove classificazioni.

La sostituzione delle voci di Titolare comporta l'impossibilità di aprire nuovi fascicoli nelle voci precedenti, a partire dalla data di attivazione delle nuove voci.

Rimane possibile registrare documenti in fascicoli già aperti con la classificazione precedente storicizzata fino alla chiusura degli stessi.

3. Conservazione dei documenti

La documentazione corrente è conservata a cura del Responsabile del procedimento, fino al trasferimento in Archivio di deposito, secondo quanto previsto dal Manuale di Gestione documentale del protocollo informatico, dei flussi documentali e degli archivi e dagli articoli del presente Piano.

I documenti analogici dell'Archivio storico e dell'Archivio di deposito sono conservati a cura della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi.

La documentazione analogica è depositata in appositi locali presso la Sede dell'Agenzia, idonei sotto

il profilo delle condizioni conservative. I documenti, i registri e i dati informatici, e i relativi fascicoli, sono conservati nell'Archivio centrale informatico dell'Agenzia fin dalla loro produzione, assicurando l'integrità, l'affidabilità, la riservatezza e la consultabilità nel tempo.

Il Responsabile della conservazione dei documenti informatici, d'intesa con il Responsabile dei dati personali e con la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi provvede, con il supporto della tecnologia disponibile, a conservare i documenti informatici e a controllare periodicamente a campione (almeno ogni sei mesi) la leggibilità dei documenti stessi, nonché a garantire la conservazione degli strumenti di descrizione, ricerca, gestione e conservazione dei documenti.

Il Responsabile della conservazione dei documenti informatici, in accordo con la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi provvede inoltre alla conservazione del software di gestione e conservazione dei documenti informatici, degli strumenti di ricerca, dei manuali operativi dei software, degli indici e dei repertori informatici formati e utilizzati nei sistemi di gestione dei documenti.

Il sistema deve altresì fornire la documentazione del software di gestione e conservazione, del sistema di sicurezza, delle responsabilità per tutte le fasi di gestione del sistema documentario, delle operazioni di conservazione dei documenti.

4. Formato dei documenti informatici

Per la predisposizione dei documenti informatici si adottano formati che possiedano requisiti di leggibilità, interscambiabilità, non alterabilità durante le fasi di accesso e conservazione, immutabilità nel tempo del contenuto e della struttura.

Si adottano i formati standard conformi ai termini di legge.

5. Censimento dei depositi documentari, delle banche dati e dei software

Annualmente, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi, in accordo con il Responsabile della conservazione dei documenti informatici, provvede ad effettuare il censimento dei depositi documentari, dei registri, delle banche dati e dei software di gestione documentale in uso nell'Agenzia, ai fini di programmare i versamenti dei documenti cartacei nell'Archivio di deposito e dei documenti informatici sui supporti di memorizzazione.

6. Copie del registro di protocollo e dell'archivio informatico

Il contenuto del registro di protocollo e dell'archivio informatico alla fine di ogni giorno è salvato su apposito supporto di memorizzazione attraverso l'apposito sistema di gestione documentale dotato dall'Agenzia, ai sensi dell'articolo 50-bis del D.Lgs. 82/05 (CAD) come modificato dal D. Lgs. n 235/10. Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata da parte delle unità di

protocollazione abilitate e comunque non oltre le quarantotto ore lavorative dal ricevimento dei medesimi, conferendo la Scheda di ricevuta protocollo.

Eccezionalmente, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi può autorizzare la registrazione in tempi successivi, fissando comunque un limite di tempo entro il quale devono essere protocollati.

Il Responsabile della conservazione dei documenti informatici, d'intesa con la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi cura la conservazione e la verifica delle copie di sicurezza.

7. Piano della fascicolazione annuale

Prima della fine dell'anno solare, la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi provvede a concordare con i Responsabili degli uffici dell'Agenzia il Piano di Fascicolazione (All. 4) per l'anno successivo, in base al Titolario di classificazione (All. 1).

Nel Piano di Fascicolazione (All. 4) sono elencati i fascicoli destinati a conservazione annuale e permanente, come indicato nel Titolario e Massimario di scarto (All.1).

L'elenco delle tipologie documentarie sottoposte a registrazione particolare viene aggiornato annualmente su iniziativa della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi. Per la documentazione soggetta a registrazione particolare si rimanda alla sezione 6 - "*Casi particolari*" - del Manuale di gestione documentale.

Durante l'anno è possibile aggiungere al Piano di fascicolazione ogni fascicolo che si renda necessario, secondo quanto stabilito dal Manuale di gestione documentale del protocollo informatico, dei flussi documentali e degli archivi.

8. Versamento dei documenti analogici nell'Archivio di deposito

Le operazioni di versamento dei documenti dell'Archivio corrente nell'Archivio di deposito e dell'Archivio di deposito nell'Archivio Storico devono essere autorizzate dalla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Ogni ufficio dell'Agenzia è tenuto a versare all'Archivio di deposito i fascicoli cartacei che corrispondono ad affari o procedimenti conclusi da un anno, nonché tutti i fascicoli annuali e i fascicoli del personale cessato.

I fascicoli relativi ad oggetti in corso di trattazione, i fascicoli conclusi nell'anno corrente e nell'anno precedente devono essere conservati presso gli uffici di appartenenza.

Prima di effettuare il trasferimento, il responsabile del procedimento, procede alla eliminazione di tutti quei documenti che non sono destinati alla conservazione quali: minute, appunti, fotocopie in eccesso,

documentazione inutile, nonché graffette, elastici e buste di plastica.

Le pubblicazioni, prodotte da altri Enti, non devono essere inviate in archivio; le pubblicazioni dell'Agenzia vanno trasmesse in un massimo di n. 3 copie e sono conservate in una apposita sezione dell'archivio.

Il soggetto versante è responsabile del buon ordine della documentazione consegnata. Per il trasferimento in Archivio di deposito si seguono le procedure di seguito riportate.

9. Procedure trasferimento documentazione in Archivio dell'Agenzia

Le richieste di trasferimento di documentazione presso l'Archivio di deposito e Storico devono pervenire alla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi corredate di:

- elenco riassuntivo della documentazione che si intende depositare, indicante contenuto e numero complessivo delle unità archivistiche;
- schede identificative di ciascuna unità archivistica (una per ogni unità trasferita), compilate a cura dell'ufficio proponente in maniera leggibile e secondo le indicazioni di cui al Modulo cod. Pr.04_Mod.02 Rev. 00 ("Modello etichetta per contenitori da trasferire presso l'Archivio di deposito") del Manuale di Gestione documentale del protocollo informatico, dei flussi documentali e degli archivi (vedi sezione 13.4 *"L'archivio di deposito"* del suddetto Manuale);
- Ove necessario, provvederà la S.S. Bilancio, Programmazione e Acquisti a definire le modalità di trasferimento del materiale a cura di eventuali apposite Ditte di facchinaggio;
- Tutti i documenti devono essere sempre raccolti in faldoni (o in equivalenti cartelle chiuse), all'esterno dei quali devono essere chiaramente indicati almeno i seguenti dati:
 - struttura produttrice;
 - natura del materiale contenuto;
 - anno/i di riferimento.

Non sarà accettata documentazione sciolta, inserita in scatole o variamente fascicolata. Qualora i faldoni, per comodità di trasporto, vengano raccolti in scatole, anche queste ultime dovranno riportare all'esterno le medesime indicazioni sopra specificate.

Non sarà accettato materiale diverso dalla documentazione amministrativa in senso stretto (es.: modulistica, materiale di cancelleria, materiale pubblicitario, arredi, oggetti, ecc...). La documentazione da archiviare deve giungere priva di quella parte di materiale che è già possibile avviare allo scarto (v. successivo punto 12 *"Procedure per lo scarto di documentazione di archivio"*).

I faldoni da trasferire, infine, devono essere per quanto possibile "compattati", evitando cioè di archiviare in faldoni di grandi dimensioni un numero esiguo di documenti e procedendo eventualmente

all'accorpamento di questi ultimi in un unico nuovo faldone.

10. Trasferimento dei documenti analogici nell'Archivio Storico

Nel rispetto del D.Lgs. 42/2004, i documenti dell'Archivio di deposito relativi agli affari esauriti da oltre quarant'anni devono essere versati all'Archivio Storico dell'Agenzia. I documenti ed i fascicoli selezionati per la conservazione permanente devono essere ordinati rispettando i criteri delineati per l'archiviazione corrente e di deposito.

È tuttavia possibile depositare in Archivio Storico anche documentazione più recente, purché non rivesta più un preminente carattere giuridico-amministrativo per l'Agenzia e sia destinata alla conservazione permanente in base al Massimario di scarto (All.1).

Nell' Archivio Storico sono inoltre conservati i fondi archivistici di Enti pubblici soppressi acquisiti dall'Agenzia.

11. Selezione e scarto dei documenti – Massimario di Scarto

Tutti i documenti privi di valore giuridico, amministrativo e storico, non ritenuti idonei alla conservazione permanente, dovranno essere sottoposti alla procedura di scarto di seguito indicata.

Le operazioni di selezione e scarto sono curate dalla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi, in collaborazione con l'ufficio produttore.

La selezione va effettuata sulla base del Titolare di Classificazione e Massimario di Scarto della documentazione del sistema Sanitario e Socio Sanitario di Regione Lombardia, che l'Agenzia adotta come proprio (All.1). Gli elenchi dei documenti proposti per lo scarto sono trasmessi alla Soprintendenza Archivistica per la Lombardia a cura della Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi per l'acquisizione del nulla osta preventivo.

La medesima Struttura cura le operazioni finalizzate alla distruzione fisica dei documenti cartacei e, in collaborazione con il Responsabile della conservazione dei documenti informatici, provvede alla rimozione dei documenti elettronici dagli archivi o dai supporti di conservazione/memorizzazione.

12. Procedure per lo scarto di documentazione di archivio

Le richieste di scarto di documentazione di Archivio di deposito devono pervenire entro il 31 marzo ed il 30 settembre di ogni anno alla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi che provvederà all'acquisizione del previsto nulla osta da parte della Soprintendenza Archivistica per la Lombardia ed alla conseguente distruzione del materiale, tramite Ditte specializzate del settore che garantiscano l'osservanza delle normative in materia.

A ciascuna richiesta dovrà essere accluso l'elenco (vedi Modulo cod. Pr.04_Mod.01 Rev. 01 "Modello

per gli atti da proporre allo scarto”) della documentazione proposta per lo scarto, da compilarsi secondo le indicazioni riportate nella sezione 13.7 *“Compilazione elenco documentazione per lo scarto”* del Manuale di Gestione documentale del protocollo informatico, dei flussi documentali e degli archivi.

Tale elenco dovrà essere inoltre trasmesso in formato elettronico alla Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi.

La valutazione sulla scartabilità o meno della documentazione dovrà essere effettuata dal Responsabile della Struttura proponente, sulla base di quanto disposto nel Massimario di scarto. Nell’eventualità che una particolare tipologia di documenti non figuri come specifica voce nel predetto Massimario, la valutazione dovrà farsi, ove possibile, per analogia.

Spetterà comunque al Responsabile dell’ufficio dell’Agenzia proponente valutare l’utilità e la rilevanza di conservazione della documentazione per la quale viene proposto lo scarto, procedendo - se del caso - a separata elencazione del materiale “dubbio”, da sottoporre al vaglio della Soprintendenza Archivistica.

Sono sempre scartabili le copie di tutti i documenti i cui originali siano conservati altrove, in archivi e/o raccolte ufficiali (es.: deliberazioni, decreti, determinazioni, note/circolari regionali, fatture, ecc.). Non è soggetto a particolari procedure di scarto - e non dovrà pertanto essere inserito negli elenchi di cui trattasi, bensì smaltito nelle forme ritenute più opportune - il materiale che non costituisce “documentazione d’archivio” in senso stretto: giornali, riviste, Gazzette Ufficiali, BURL, modulistica in bianco, depliant, materiale pubblicitario, di cancelleria, ecc.

13. Esternalizzazione

Nel caso in cui l’Agenzia affidi a terzi, in tutto o in parte la conservazione dei documenti, sia analogici sia informatici, è necessario accertarsi che il fornitore esibisca adeguate certificazioni di capacità tecnico-scientifica, dichiarando espressamente di svolgere il servizio secondo la normativa vigente e mediante procedure tecniche dettagliatamente descritte nel disciplinare di incarico e specificamente disciplinate in apposita convenzione.

La Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi deve curare che le procedure di outsourcing avvengano d’intesa con la competente Soprintendenza archivistica.

14. Aggiornamento

Ogni anno la Struttura competente del protocollo informatico, della gestione dei flussi documentali e degli archivi, d’intesa con il Responsabile della Conservazione dei documenti informatici, valuta la congruità del presente Piano e provvede agli eventuali aggiornamenti, dandone comunicazione agli uffici dell’Agenzia.

FASCICOLI ANNUALI

Amministrazione Generale

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.1.01	Normativa/ provvedimenti	Normativa statale, regionale, pareri, circolari, direttive, delibere di altri enti, Comunicazioni da Regione Lombardia
1.1.02	Programmazione, disposizioni, indirizzi ed obiettivi Agenzia, atti di organizzazione	Disposizioni, comunicazioni e convocazioni a carattere transitorio (convocazioni, inviti...) Deleghe di funzioni, di attività, di firma, Progetto RAR, progetti speciali
1.1.04	Controlli interni ed esterni	Controlli interni: controllo di gestione, contabilità analitica, audit interni, controllo di regolarità formale e contabile, report di controllo
1.1.05	Sistema Qualità e Risk Management	Documenti relativi al sistema di gestione per la qualità (Verballi audit ISO, procedure di Agenzia certificati ISO, Customer Satisfaction)
1.1.06	Progetti di ricerca	Progetti di ricerca regionali e/o dell'Agenzia, progetti comunitari
1.1.08	Politiche e interventi per le pari opportunità	Politiche sulle pari opportunità compresi convegni, congressi, questionari

Attività Giuridico - Legale

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.3.01	Pareri, Informative giuridiche ed attività tecnico- legali	Pareri legali/pareri giuridici e relazioni tecniche

Risorse Umane

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.4.01	Dotazione organica e gestione del personale	Piante organiche personale Agenzia, Organigrammi funzionali, Schede anagrafiche sintetiche dei dipendenti, Atti relativi alla dotazione organica
1.4.02	Concorsi e selezioni	Domande ammissioni concorsi e incarichi, documentazione accessoria concorsi e selezioni (Documenti nomina commissioni, schede di valutazione, verbali, ecc...), CV dei partecipanti
1.4.06	Retribuzioni e compensi	Documentazione contabile relativa ai comandi, trasferimenti, mobilità (trasferte, missioni), gestione buoni pasto, CUD, deleghe sindacali, cedolini mensili e retribuzioni
1.4.07	Trattamenti fiscali, contributivi e assicurativi	Pratiche assicurative per infortunio
1.4.09	Presenze assenze	Documenti relativi permessi orari, assenze, congedi, ferie, cartellini, scioperi Avvisi al personale dipendente, comunicazione indizione/adesione sciopero Permessi 150 ore

		Riepilogo timbrature personale Certificati di malattia personale
1.4.13	Formazione e aggiornamento del personale	Documentazione relativa ad attività formative interna, esterna e a distanza Avvisi eventi formativi, Incarichi docenti, Autorizzazione corsi formativi Piano annuale della formazione

Risorse finanziarie e gestione contabile

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.5.01	Attività finanziaria e contabile	Budget di cassa (rendiconto finanziario) Ordinativi/Distinte di incasso e di pagamento, documentazione relativa alla gestione della spesa (impegno, liquidazione, ordinazione e pagamento) e altre registrazioni contabili di carattere transitorio (Mandati/Reversali, movimenti del Tesoriere, ecc.) Ricognizione BES Convenzioni, attivazione e cessazione con istituti di credito Servizi bancari telematici (internet banking) Estratti conto operazioni bancarie
1.5.02	Bilancio e Rendicontazione	Budget Gestori di spesa, Bilancio: carteggio interlocutorio interno, assegnazione budget, ecc. Situazione contabili periodiche (CET)
1.5.03	Gestione entrate-uscite	Documentazione varie inerenti al flusso degli incassi (avvisi di riscossione, distinti versamenti su c/c) Cartelle pagamenti esattoriali Fatture emesse e fatture ricevute Solleciti di pagamento Rimborso spese non dovute Cessioni del credito
1.5.04	Gestione fiscale e imposte	Documenti relativi a imposte e tasse dell'Agenzia quale sostituto di imposte IRES, IRPEF, bollo virtuale, ecc. Certificazione ritenute d'acconto Modello 770 (dichiarazione sostituti d'imposta) Modello Unico (redditi IRAP e IVA)

Gestione e organizzazione del patrimonio

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.6.03	Acquisizione e gestione di beni mobili/generi di consumo e di servizi	Documentazione relativa all'acquisizione e fornitura dei beni mobili, di materiale e attrezzature tecniche, scientifiche, e non, e per la fornitura di servizi, compresi contratti RCA auto (richieste partecipazione a gare, bandi gara, offerte, verbali seduta, atti indizione e aggiudicazione, contratti, ecc.). Inventario beni mobili: Libro cespiti ammortizzabili e trasferimenti interni beni inventariati DURC Utenze varie (telefono) Lettere buoni pasto (rapporti con il fornitore)
1.6.04	Manutenzione ordinaria, straordinaria,	Contratti di manutenzione, esiti delle manutenzioni.

	ristrutturazione destinazione d'uso	
1.6.06	Sicurezza degli ambienti di lavoro	Documentazione dei Rappresentanti Lavoratori Sicurezza (RLS), procedure 1° soccorso, gestione e valutazione del rischio, piani per la sicurezza dei luoghi di lavoro, nomina dei responsabili per la sicurezza, formazione specifica del personale dipendente.
Sistemi Informativi e Comunicazione		
<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.7.01	Sistema documentale	Albo on line e pubblicazioni sul sito web ACSS relativamente alle leggi in materia di accesso e trasparenza nella pubblica amministrazione
1.7.01	Sistema documentale	Richieste di accesso ai documenti Documenti accesso civico
1.7.02	Rapporti con il pubblico, sportelli informativi e trasparenza	Segnalazioni cittadini, pubbliche relazioni, richieste informazioni, rassegna stampa, comunicazione con i media, Documenti relativi alla rappresentanza istituzionale (eventi, inviti, ecc)
1.7.03	Tutela della riservatezza	Aggiornamenti elenchi incaricati privacy, nomina incaricati, Informativa dell'Agenzia e consenso al trattamento dati
1.7.04	Biblioteche e centri di documentazione	Documentazione relativa al servizio SBBL, acquisti, catalogazione, richieste di consultazione e prestito, ecc...
1.7.05	Sistema informatico, reti e sicurezza	Abilitazione ai dipendenti all'uso dei sistemi informatici dell'Agenzia
Area sanitaria e sociosanitaria territoriale		
Governo sanitario e sociosanitario		
<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
2.7.02	Osservatorio epidemiologico	Indagini e statistiche demografiche ed epidemiologiche ¹

¹ Fonte: **Titolario e Massimario del Sistema Sociosanitario lombardo** già Sistema Sanitario e Sociosanitario di Regione Lombardia.
Revisione 04.

FASCICOLI PERMANENTI

Amministrazione Generale

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.1.02	Programmazione, disposizioni, indirizzi ed obiettivi aziendali, atti di organizzazione	Atti e provvedimenti emessi dall'Ente originali (Deliberazioni, Determinazioni DG, Determinazioni di S.C.), Regolamenti, Piani strategici ACSS (PIAO), atti organizzativi ACSS, Piano dei Controlli e dei Protocolli Quadro
1.1.03	Protocolli di intesa, convenzioni con Enti pubblici e privati no profit	Convenzioni, Collaborazioni e Accordi Quadro con istituzioni varie
1.1.04	Controlli interni ed esterni	Controlli esterni: ispezioni, verifiche di enti terzi (Corte dei Conti, Ministero della Salute, ecc.)
1.1.07	Associazioni di Volontariato e tutela dei diritti del malato	Rapporti con il mondo associativo e del no-profit

Organi e Organismi

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.2.01	Legale Rappresentante	Atto nomina DG, atti inerenti, compiti, rinnovo, cessazione
1.2.02	Organismi direttivi e scientifici	Atto Nomina Comitato di Direzione, atti inerenti, compiti, rinnovo, cessazione
1.2.03	Organismi di controllo interno ed esterno	Documenti Trasparenza e Prevenzione Corruzione, Segnalazioni Whistleblower, Documentazione relativa al Nucleo di Valutazione (NVP), Documenti relativi al Collegio Sindacale

Attività Giuridico - Legale

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.3.02	Contenzioso Legale	Procedimento civile, penale, amministrativo, giusvaloristico e stragiudiziale (sentenze, ordinanze, ricorsi, comunicazioni tra le parti e i legali, querele all'Autorità Giudiziaria, denunce)
1.3.03	Procedure concorsuali ed esecutive	Avvisi di apertura pratica assicurativa per danni, richieste di risarcimento
1.3.04	Assicurazioni e gestione sinistri	Denunce di sinistro, atti legali per controversie su risarcimenti, Documentazione per i sinistri, polizze assicurative attive (furto, incendio, infortuni)

Risorse Umane

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.4.02	Concorsi e selezioni	Bandi di concorso, Atto di indizione, Avvisi di mobilità, Verbali commissione esaminatrice, Graduatoria idonei, Atto approvazione graduatoria
1.4.03	Assunzioni, inquadramenti, incarichi e cessazione	Certificati di servizio, Certificati di stipendio, Documenti relativi mobilità interna/esterna del professionista, Documenti periodo di prova, autorizzazioni per incarichi esterni, comunicazioni relative alla variazione dati personali, opzione regime di impegno a tempo

		pieno o a tempo parziale
1.4.04	Istituti contrattuali sospensivi della prestazione lavorativa	Documentazione relativa alle aspettative, Documentazione relativa ai comandi entrata/uscita
1.4.05	Organizzazioni sindacali e contrattazione	Documenti legati ai rapporti con le rappresentanze sindacali, comunicazioni elezione RSU e relativa documentazione (verbali, incontri, indizione assemblee)
1.4.07	Trattamenti fiscali, contributivi e assicurativi	Trattamenti fiscali e contributivi del personale, (INPS) Trattamento di fine rapporto/servizio (TFR)
1.4.08	Inabilità al lavoro, invalidità, infermità, indennizzo	Dichiarazione infermità per cause di servizio/ malattie professionali
1.4.12	Valutazione del personale	Procedimenti disciplinari, scheda di valutazione del professionista, segnalazioni/ comunicazioni sull'inosservanza dei doveri d'ufficio
1.4.13	Formazione e aggiornamento del personale	Attestati di corsi di formazione del personale
1.4.14	Deontologia professionale ed etica del lavoro	Codice Etico, Codice di Comportamento, iniziative di prevenzione in materia di anticorruzione.
1.4.15	Personale non strutturato o convenzionato	Pratiche di affidamento di incarichi di lavoro autonomo (incarichi libero professionali, incarichi di natura occasionale, Borse di studio, Richieste a professionisti esterni per pareri tecnici per gare ecc... Documenti relativi alla presa servizio e alla cessazione di personale atipico (collaboratori, stagisti, specializzandi, tirocinanti)

Risorse finanziarie e gestione contabile

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.5.01	Attività finanziaria e contabile	Verbali e verifiche di cassa (Gestione Cassa economale) Registri contabili principali, anche sotto forma di banche dati (Mastro, Giornali di Cassa, ecc.)
1.5.02	Bilancio e Rendicontazione	Conto Giudiziale, Percorso Certificabilità del Bilancio (PAC) Libro cespiti

Gestione e organizzazione del patrimonio

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.6.03	Acquisizione e gestione di beni mobili/generi di consumo e servizi	Gestione parcheggi interni

1.6.06	Sicurezza degli ambienti di lavoro	Sorveglianza sanitaria e sicurezza ambiente di lavoro (verbali di sopralluogo) Visite mediche del personale e attestazione di idoneità

Sistemi Informativi e Comunicazione

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
1.7.01	Sistema documentale	Documentazione relativa al sistema di gestione documentale e del servizio archivistico (manuale di gestione documenti, gestione del protocollo, gestione degli archivi, procedure di scarto, titolari, massimari, richieste di consultazione, Rapporto giornaliero Amministrativo del servizio Larchive)
1.7.02	Rapporti con il pubblico, sportelli informativi e trasparenza	Piano di Comunicazione
1.7.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla gestione delle banche dati (es. sistema di gestione del personale, sistema finanziario-contabile, ecc) Documentazione relativa alla sicurezza informatica
1.7.06	Statistiche e reporting	Statistiche e report istituzionali (es. flussi regionali, Questionari ISTAT, ecc) a fronte di richieste di enti esterni

Area sanitaria e sociosanitaria territoriale

Prevenzione e sicurezza negli ambienti di lavoro

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
2.2.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività per la prevenzione e sicurezza negli ambienti di lavoro
2.2.03	Igiene e sicurezza sul lavoro	Attività di vigilanza sanitaria sull'applicazione delle norme in materia di sicurezza ed igiene del lavoro negli ambienti di lavoro (segnalazioni, denunce, verbali di sopralluogo, verbale sanzionatorio, ecc.) Inchiesta infortuni (comprendente denunce, relazione di sopralluogo, esecuzione di rilievi, certificato medico di infortunio lavorativo)

Governo sanitario e sociosanitario

<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
2.7.03	Flussi informativi sanitari e sociosanitari	Flussi dalle ATS Flussi informativi Ministeriali, regionali, altri enti
2.7.04	Accreditamento e controllo strutture sanitarie	Documentazione relativa a vigilanza/controllo accreditamento: Verbali di controllo e sanzionatorio, segnalazioni, diffide amministrative strutture sanitarie
2.7.05	Autorizzazione e controllo strutture sociosanitarie	Documentazione relativa a vigilanza/controllo accreditamento: Verbali di controllo e sanzionatorio, segnalazioni, diffide amministrative strutture sociosanitarie
2.7.06	Acquisto e controllo	Verbali di controllo e sanzionatori su esiti ricoveri e prestazioni ambulatoriali delle strutture sanitarie

	prestazioni sanitarie	
2.7.07	Acquisto e controllo prestazioni socio sanitarie	Verbali di controllo e sanzionatori su esiti e prestazioni ambulatoriali delle strutture socio sanitarie
Area ospedaliera		
Medicina del Lavoro		
<u>Classe</u>	<u>Sottoclasse</u>	<u>Descrizione</u>
3.10.01	Cartella sanitaria e di rischio del lavoratore	Cartella sanitaria e di rischio del lavoratore
3.10.02	Malattia professionale e infortunio sul lavoro	Documenti relativi alla Malattia professionale e infortunio sul lavoro (Registri vaccinazioni, Registri infortuni...) ²

² Fonte: **Titolario e Massimario del Sistema Socio sanitario lombardo** già Sistema Sanitario e Socio sanitario di Regione Lombardia.
Revisione 04.

IL COMITATO DI DIREZIONE

**DELIBERAZIONE N. 07
DEL 21/09/2022**

**OGGETTO: APPROVAZIONE REGOLAMENTO PER L'ESERCIZIO DEL
DIRITTO DI ACCESSO AI DOCUMENTI AMMINISTRATIVI E DEL DIRITTO DI
ACCESSO CIVICO SEMPLICE E GENERALIZZATO.**

Coordinatore: Dott. Giovanni Bladelli

Componente: Dott. ssa Loredana Luzzi

Componente: Dott. Marino Nonis

PREMESSO

- che il diritto di accesso agli atti, alle informazioni e dai dati detenuti dalla Pubblica Amministrazione, attese le sue rilevanti finalità di pubblico interesse, costituisce principio generale dell'attività amministrativa, al fine di favorire la partecipazione e di assicurare l'imparzialità nella trasparenza;
- che l'ordinamento giuridico, in materia di accesso, prevede distinti istituti:
 - l'accesso documentale di cui agli artt. 22 e seguenti della L. n. 241/1990, riconosciuto ai soggetti che dimostrino di essere titolari di un "interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso";
 - l'accesso civico semplice, previsto dall'art. 5 co. 1 del D. Lgs. n. 33/2013, riconosciuto a chiunque, indipendentemente dalla titolarità di una situazione giuridica soggettiva connessa, circoscritto ai solo atti, documenti e informazioni oggetto di obblighi di pubblicazione;
 - l'accesso civico generalizzato disciplinato dall'art. 5 co. 2 e dall'art. 5-bis del decreto trasparenza, anch'esso a titolarità diffusa, avente ad oggetto tutti i dati, i documenti e le informazioni detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli per i quali è stabilito un obbligo di pubblicazione, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti;

RICHIAMATA la deliberazione dell'Autorità Nazionale Anticorruzione (ANAC) n. 1309 del 28 dicembre 2016, adottata ai sensi del comma 6, art. 5-bis, del D. Lgs. n. 33/2013, avente ad oggetto "Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del D. Lgs 33/2013", la quale prevede l'adozione, da parte delle singole amministrazioni, di un apposito regolamento interno sull'accesso ai documenti, ai dati e alle informazioni, che fornisca un quadro organico e coordinato dei profili applicativi relativi alle diverse tipologie di accesso;

RITENUTO di adottare un regolamento unitario, per la disciplina dei diversi istituti previsti dall'ordinamento, per l'accesso ai documenti, ai dati ed alle informazioni detenute dall'Agenzia di Controllo del Sistema Sociosanitario Lombardo (ACSS);

SU CONFORME PROPOSTA del Dirigente Responsabile della SSD Trasparenza Avv. Elisa Maria Rottoli che dichiara la legittimità e la regolarità tecnica del presente provvedimento;

A VOTI UNANIMI

DELIBERA

per le motivazioni formulate in premessa, che qui s'intendono integralmente riportate:

1. di approvare il Regolamento per l'esercizio del diritto accesso agli atti, ai documenti amministrativi e del diritto di accesso civico semplice e generalizzato, dell'Agenzia di Controllo del Sistema Sociosanitario Lombardo (ACSS), allegato al presente provvedimento quale parte integrante e sostanziale;
2. di dare atto che il presente provvedimento non comporta oneri di spesa;
3. di dare mandato al Dirigente Responsabile della SSD Trasparenza per tutti i successivi adempimenti di attuazione del presente provvedimento, ai sensi dell'art. 6 della L. n. 241/1990;
4. di dare atto che il presente provvedimento è immediatamente esecutivo ai sensi del comma 6 dell'art. 17 della L.R. 33/2013 (come modificato dalla L.R. 23/2015);

Componente Coordinatore
Dr. Giovanni Bladelli

Componente
Dr.ssa Loredana Luzzi

Componente
Dr. Marino Nonis

Atto firmato digitalmente ai sensi delle vigenti disposizioni di legge

ALLEGATO N. 1 alla deliberazione n. 7 del 21/09/2022

Agenzia di Controllo del Sistema Sociosanitario Lombardo

REGOLAMENTO PER L'ESERCIZIO DEL DIRITTO DI ACCESSO AI DOCUMENTI AMMINISTRATIVI E DEL DIRITTO DI ACCESSO CIVICO SEMPLICE E GENERALIZZATO

Rev.	Approvato con:	N.	DATA	Descrizione
1	Deliberazione del Comitato di Direzione	7	21/09/2022	Approvazione

SOMMARIO

SEZIONE I – PRINCIPI GENERALI	3
1. OGGETTO.....	3
2. DEFINIZIONI	3
3. RESPONSABILE DEL PROCEDIMENTO E STRUTTURA DI SUPPORTO IN MATERIA DI ACCESSO	5
4. REGISTRO DELLE RICHIESTE DI ACCESSO	6
5. PUBBLICAZIONI SUL SITO ISTITUZIONALE E MODULISTICA PER L'UTENZA.....	6
SEZIONE II – DIRITTO DI ACCESSO AI DOCUMENTI AMMINISTRATIVI.....	7
6. TITOLARITÀ DEL DIRITTO DI ACCESSO AI SENSI DELLA L. N. 241/1990	7
7. OGGETTO DEL DIRITTO DI ACCESSO	7
8. MODALITÀ DI ESERCIZIO.....	8
9. ACCESSO INFORMALE	8
10. ACCESSO FORMALE	8
11. COMPITI DEL RESPONSABILE DEL PROCEDIMENTO	9
12. TERMINI PROCEDIMENTALI	10
13. CONCLUSIONE DEL PROCEDIMENTO CON ACCOGLIMENTO DELLA RICHIESTA	10
14. CONCLUSIONE DEL PROCEDIMENTO CON PROVVEDIMENTO DI DINIEGO	11
15. DIFFERIMENTO DEL DIRITTO DI ACCESSO	13
16. CONTROVERSIE RELATIVE ALL'ACCESSO.....	13
17. NORMATIVE SPECIALI IN MATERIA DI ACCESSO	13

SEZIONE III – DIRITTO DI ACCESSO CIVICO SEMPLICE.....	15
18. PRINCIPI E OGGETTO DELL'ACCESSO CIVICO SEMPLICE.....	15
19. LEGITTIMAZIONE ALL'ACCESSO.....	15
20. MODALITÀ DI ESERCIZIO.....	15
21. ISTRUTTORIA E CONCLUSIONE DEL PROCEDIMENTO.....	16
22. RICORSI.....	16
SEZIONE IV – DIRITTO DI ACCESSO CIVICO GENERALIZZATO	17
23. PRINCIPI E OGGETTO DEL DIRITTO DI ACCESSO CIVICO GENERALIZZATO	17
24. SOGGETTI LEGITTIMATI	17
25. MODALITÀ DI ESERCIZIO	17
26. ADEMPIMENTI ISTRUTTORI DEL RESPONSABILE DEL PROCEDIMENTO	18
27. TERMINI PROCEDIMENTALI	19
28. CAUSE TASSATIVE DI ESCLUSIONE DELL'ACCESSO	19
29. LIMITI RELATIVI ALL'ESERCIZIO DEL DIRITTO DI ACCESSO CIVICO GENERALIZZATO	20
30. ACCOGLIMENTO DELLA RICHIESTA DI ACCESSO GENERALIZZATO.....	22
31. DINIEGO, LIMITAZIONE E DIFFERIMENTO.....	22
32. RIESAME DEI PROVVEDIMENTI ADOTTATI.....	22
33. RICORSI.....	23
SEZIONE V – NORME FINALI	24
34. NORME DI RINVIO ED ENTRATA IN VIGORE.....	24
35. MODULISTICA	24

SEZIONE I

PRINCIPI GENERALI

1. OGGETTO

1. Il presente Regolamento disciplina, in un quadro organico e unitario, le diverse tipologie di accesso previste dall'ordinamento, nel rispetto del principio della libertà di accesso alle informazioni – cosiddetta "Freedom of Information Act" (FOIA) – di cui alla Convenzione Europea dei Diritti dell'Uomo (CEDU), nonché delle disposizioni del Regolamento (UE) n. 2016/679 e del D. Lgs. n. 196/2003, in materia di protezione dei dati personali e della riservatezza delle persone fisiche.

2. La normativa vigente prevede tre istituti di cui è possibile avvalersi per accedere ai documenti, alle informazioni e ai dati detenuti dalla Pubblica Amministrazione:

- **accesso ai documenti amministrativi**: si tratta dell'accesso agli atti previsto dalla L. n. 241/1990 e dal D.P.R. n. 184/2006, c.d. "accesso documentale", di cui possono avvalersi i soggetti portatori di un interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso, per prendere visione ed estrarre copia di documenti amministrativi (cfr. **Sez. II**);
- **accesso civico semplice**: si riferisce al diritto di accesso ai dati ed ai documenti oggetto di pubblicazione obbligatoria sul sito istituzionale dell'ente, nei casi in cui sia stata omessa la loro pubblicazione, come previsto dall'art. 5, comma 1, del D.Lgs. n. 33/2013 (cfr. **Sez. III**);
- **accesso civico generalizzato**: si riferisce alla possibilità di accedere a dati, documenti e informazioni detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria, senza la necessità di indicare motivazioni, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, secondo quanto previsto dagli artt. 5 c. 2 e 5-bis del D.Lgs. n. 33/2013 (cfr. **Sez. IV**).

2. DEFINIZIONI

1. Ai fini del presente regolamento si intende per:

- **Documento amministrativo**: ogni rappresentazione grafica, fotografica, cinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale (art. 22, c. 1, lett. d), L. n. 241/1990);

- Dato: elemento conoscitivo di base, indipendentemente dal supporto fisico su cui è incorporato e a prescindere dai vincoli derivanti dalle sue modalità di organizzazione e conservazione;
- Informazione: rielaborazione di dati detenuti dall'Agenzia, effettuata per propri fini e contenuta in distinti documenti;
- Dati personali: qualsiasi dato o informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 n. 1 Reg. UE 2016/679);
- Dati rientranti in particolari categorie: si tratta dei c.d. "dati sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, o dati relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (art. 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- Dati relativi a condanne penali e reati: si tratta dei c.d. "dati giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (art. 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
- Trattamento dei dati: Trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali. I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.
- Interessati all'accesso documentale: tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse, diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso (art. 22, c. 1, L. n. 241/1990);
- Interessati all'accesso civico: chiunque, senza alcuna limitazione, voglia accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni (art. 5, commi 1, 2 e 3, D.Lgs n. 33/2013);
- Controinteressati: tutti i soggetti, individuati o facilmente individuabili in base alla natura dell'istanza, che dall'esercizio del diritto di accesso potrebbero vedere pregiudicato il loro diritto alla riservatezza o, per l'accesso civico generalizzato, che potrebbero subire un pregiudizio concreto alla tutela di uno dei seguenti interessi privati: protezione dei dati personali, libertà e segretezza della corrispondenza, interessi economici e commerciali, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali (art. 5 c. 5 e art. 5-bis c. 2, D.Lgs. n. 33/2013).

3. RESPONSABILE DEL PROCEDIMENTO E STRUTTURA DI SUPPORTO IN MATERIA DI ACCESSO

1. Il Responsabile del procedimento di accesso documentale e civico generalizzato è il Dirigente della Struttura, complessa, semplice o semplice dipartimentale, competente per materia (cfr. art. 6, c. 6, DPR n. 184/2006, che indica quale responsabile il dirigente o il funzionario preposto all'unità organizzativa competente a formare o a detenere stabilmente la documentazione richiesta).

Per i procedimenti di accesso civico semplice, il Responsabile del Procedimento coincide con il Responsabile della Prevenzione della Corruzione e della Trasparenza.

2. Al Responsabile del procedimento competono tutti gli adempimenti istruttori necessari in relazione all'istanza di accesso ricevuta. In particolare, il Responsabile del procedimento, per la relativa attuazione, può richiedere la collaborazione della Struttura di ACSS individuata quale centro di competenza per l'accesso agli atti previsto dalla Circolare n. 2/2017 del Ministero per la Semplificazione e la Pubblica Amministrazione (cfr. deliberazione ANAC n. 1309 del 28 dicembre 2016 e art. 5-bis, c. 6, D.Lgs. n. 33/2013), per avere il supporto relativo agli adempimenti istruttori.

3. La fase istruttoria comprende i seguenti adempimenti:

- valutazione circa le condizioni di ammissibilità dell'istanza, i requisiti di legittimazione del richiedente ed i presupposti rilevanti ai fini dell'emanazione del provvedimento conclusivo (cfr. successive sezioni del presente regolamento);
- eventuale trasmissione dell'istanza ad altro Ente, individuato come competente;
- eventuale richiesta di integrazione dell'istanza di accesso, nel caso in cui la stessa sia incompleta;
- accertamento circa l'esistenza di eventuali soggetti controinteressati;
- invio delle comunicazioni e notificazioni previste dalle leggi e dai regolamenti;
- redazione del provvedimento conclusivo del procedimento e comunicazione all'interessato (con acquisizione delle ricevute di consegna).

4. Qualora l'Agenzia riceva una richiesta di accesso priva dell'indicazione della tipologia (accesso documentale / civico generalizzato / civico semplice) il Responsabile del Procedimento, ove l'istante non integri la richiesta con la relativa specifica, può provvedere direttamente alla qualificazione dell'istanza.

In particolare, possono essere applicati i seguenti criteri:

- discrimine accesso documentale / accesso civico (semplice o generalizzato): il principale criterio di demarcazione concerne l'oggetto dell'istanza e l'eventuale interesse sotteso, che nell'accesso documentale deve essere personale e motivato. L'accesso civico ha invece lo scopo di favorire forme diffuse di controllo sull'azione amministrativa e sul perseguimento delle funzioni istituzionali e comporta la successiva conoscibilità al pubblico dei documenti e dei dati consegnati. Per tale motivo, se vengono richiesti documenti e dati relativi a posizioni individuali e specifiche, è necessaria l'osservanza dei requisiti richiesti dalla legge per l'accesso documentale.

- discrimine accesso civico semplice / accesso civico generalizzato: occorre verificare se quanto richiesto è soggetto ad obbligo di pubblicazione sul sito istituzionale. L'accesso civico semplice, al contrario di quello generalizzato, costituisce un rimedio alla mancata osservanza degli obblighi di pubblicazione previsti dal D.Lgs. n. 33/2013 o da normative di settore.
5. Il Responsabile del procedimento, nel rispetto di quanto previsto dall'art. 6-bis della L. n. 241/1990 e dalle disposizioni del D.P.R. n. 62/2013, ha l'obbligo di astenersi in caso di conflitto di interessi e, correlativamente, l'obbligo di segnalare al dirigente sovraordinato ogni situazione di conflitto anche potenziale.
6. Il Responsabile del procedimento e i dipendenti eventualmente coinvolti, a qualunque titolo, nella fase istruttoria del procedimento di accesso, sono tenuti all'osservanza del segreto d'ufficio nei rapporti con i colleghi e con i terzi.

4. REGISTRO DELLE RICHIESTE DI ACCESSO

1. Presso ACSS è istituito il cosiddetto "Registro degli accessi" ad atti, dati e documenti, secondo quanto previsto dalle Linee guida approvate dall'Autorità Nazionale Anticorruzione con deliberazione n. 1309 del 28 dicembre 2016.

Il registro, tenuto dal Responsabile della Prevenzione della Corruzione e della Trasparenza, contiene l'elenco delle richieste pervenute all'Agenzia, con l'indicazione della tipologia di accesso, della data di presentazione/protocollo, dell'oggetto e del relativo esito, nonché di eventuali note, e viene aggiornato per ogni semestre di riferimento, tramite pubblicazione nella sezione Amministrazione trasparente, "altri contenuti- accesso civico" del sito web istituzionale. A tal fine, ogni Struttura è tenuta a monitorare i procedimenti di accesso di propria competenza, formali e informali, di ogni tipologia, e a rendicontarli al termine di ogni semestre al Responsabile della Prevenzione della Corruzione e della Trasparenza.

5. PUBBLICAZIONI SUL SITO ISTITUZIONALE E MODULISTICA PER L'UTENZA

1. I provvedimenti degli organi di vertice e le determinazioni dirigenziali, nonché i dati soggetti a pubblicazione obbligatoria ai sensi del D.Lgs. n. 33/2013, sono pubblicati nel sito istituzionale di ACSS, nell'Albo Pretorio online e nella sezione Amministrazione Trasparente, nei modi e nelle forme previste dalla legge, con particolare riferimento agli adempimenti in materia di trasparenza e pubblicità all'interno delle pubbliche amministrazioni.

2. Ai fini dell'attuazione delle diverse tipologie di diritto d'accesso è resa reperibile, sul sito web istituzionale, nella sezione Amministrazione Trasparente > Altri Contenuti > Accesso Civico la modulistica occorrente per presentare le istanze.

SEZIONE II

DIRITTO DI ACCESSO AI DOCUMENTI AMMINISTRATIVI

6. TITOLARITÀ DEL DIRITTO DI ACCESSO AI SENSI DELLA L. N. 241/1990

1. Per diritto di accesso ai documenti amministrativi si intende la situazione giuridicamente rilevante e tutelata degli interessati di prendere visione e/o di richiedere copia dei documenti amministrativi formati o detenuti stabilmente da ACSS. Tale diritto riveste rilevante finalità di pubblico interesse e costituisce principio generale dell'ordinamento giuridico, nell'ottica di favorire la partecipazione e di assicurare la trasparenza e l'imparzialità dell'azione amministrativa.
2. La titolarità del diritto di accesso ai documenti amministrativi è riconosciuta ai soggetti interessati, ai sensi dell'art. 10 e degli artt. 22 ss. della L. n. 241/1990. Il diritto di accesso in favore di associazioni e comitati portatori di interessi collettivi o diffusi è consentito previo accertamento della legittimazione e della natura dell'interesse giuridico di cui sono portatori, stabiliti da una norma o indicati nello statuto.
3. L'acquisizione da parte di soggetti pubblici di documenti amministrativi si informa al principio di leale cooperazione istituzionale (cfr. comma 5 art. 22 L. 241/1990).
4. È estraneo alla disciplina dell'accesso agli atti ed è sempre consentito l'accesso alla documentazione su disposizione dell'Autorità Giudiziaria o di Polizia, previa presentazione di specifica richiesta scritta.

7. OGGETTO DEL DIRITTO DI ACCESSO

1. Oggetto del diritto di accesso sono i documenti amministrativi materialmente esistenti al momento della richiesta e detenuti da ACSS, che il richiedente ha l'onere di individuare specificamente o di rendere facilmente individuabili da parte dell'Agenzia. L'istituto dell'accesso agli atti documentale, al contrario di quello civico, non consente la comunicazione di informazioni o di meri dati che non abbiano forma di documento amministrativo (fatto salvo quanto previsto dall'art. 15 del Regolamento UE 2016/679 in materia di accesso dell'interessato ai dati personali che lo riguardano).
2. Non sono ammissibili richieste di accesso generiche, massive o preordinate ad un controllo generalizzato dell'operato della PA, né ACSS è tenuta a rielaborare i documenti e i dati in suo possesso, o a predisporre ulteriore documentazione, al fine di soddisfare le richieste di accesso pervenute, in base al principio di non aggravamento dell'azione amministrativa.
3. Ai sensi dell'art. 16 della L.R. n. 1/2012, il diritto di accesso può essere esercitato in qualunque tempo, indipendentemente dalla cessazione dell'obbligo di detenzione da parte dell'amministrazione, sempre che l'Ente detenga ancora il documento e che sussista l'attualità dell'interesse del richiedente.

8. MODALITÀ DI ESERCIZIO

1. L'istanza di accesso agli atti deve essere presentata dal soggetto interessato o da suo delegato, unitamente a copia dei documenti di identità, e deve essere motivata. Coloro che presentano una richiesta di accesso per conto di enti, persone giuridiche, associazioni o altri organismi, devono qualificarsi quali legali rappresentanti degli stessi, ovvero dichiarare la carica ricoperta o la funzione svolta che legittimi l'esercizio del diritto per conto dei soggetti rappresentati.

La legittimazione e l'interesse diretto e qualificato devono essere esplicitati chiaramente ed eventualmente comprovati mediante allegazione di idonea documentazione.

2. Il diritto di accesso viene esercitato di norma in via formale, presentando richiesta scritta sull'apposita modulistica predisposta dall'amministrazione (cfr. art. 10). Nei limitati casi di cui al successivo art. 9, la richiesta di accesso agli atti può essere presentata in via informale e riscontrata da ACSS con immediatezza.

9. ACCESSO INFORMALE

1. La richiesta di accesso informale, che può essere formulata oralmente all'ufficio di ACSS competente a formare il documento o a detenerlo stabilmente, viene prontamente valutata dal Responsabile del Procedimento, o dal funzionario delegato, e risulta ammissibile solo nei casi in cui la documentazione richiesta sia immediatamente reperibile, non vi siano soggetti controinteressati e non vi siano dubbi:

- sull'identità del richiedente;
- sugli eventuali poteri di rappresentanza (delega, procura, etc);
- sulla legittimazione e sulla sussistenza dell'interesse diretto e qualificato;
- sull'individuazione e sull'accessibilità del documento richiesto.

2. In caso di accoglimento, l'interessato può prendere visione o ricevere copia dei documenti, preferibilmente in formato elettronico.

3. Il Responsabile provvede al monitoraggio degli accessi informali, includendoli nella rendicontazione semestrale per la compilazione del Registro degli Accessi.

4. Qualora il Responsabile ritenga che l'istanza non sia ammissibile in via informale, per la necessità di approfondimenti istruttori o per la presenza di soggetti controinteressati, invita il richiedente a presentare richiesta di accesso formale.

10. ACCESSO FORMALE

1. Il diritto di accesso documentale si esercita in via formale indirizzando ad ACSS, all'attenzione del Responsabile dell'Unità Operativa competente, ove nota, un'apposita richiesta scritta, redatta sulla modulistica reperibile sul sito istituzionale dell'Agenzia, trasmessa preferibilmente via PEC all'indirizzo

acss@pec.regione.lombardia.it, oppure tramite posta ordinaria o elettronica, agli indirizzi indicati sul sito istituzionale.

2. Le istanze ricevute vengono protocollate e assegnate in competenza alla Struttura che ha prodotto o detiene la documentazione richiesta, ed in conoscenza alla Struttura individuata dagli atti aziendali vigenti quale centro di competenza in materia di accesso agli atti.

3. Qualora la richiesta sia di competenza di un'altra Pubblica Amministrazione, l'istanza formale deve essere trasmessa all'ente competente, dandone contestuale comunicazione al richiedente.

11. COMPITI DEL RESPONSABILE DEL PROCEDIMENTO

1. Il Responsabile del procedimento adotta il provvedimento finale, all'esito dei seguenti adempimenti istruttori:

- a) accertamento della propria competenza per materia, con riferimento alla documentazione richiesta;
- b) verifica dei requisiti dell'istanza, ed in particolare:
 - identità e legittimazione del richiedente, verificando che sia stata allegata copia della carta d'identità e dell'eventuale ulteriore documentazione necessaria (es.: delega all'avvocato da parte del proprio assistito, atto giudiziale di nomina del tutore, statuto delle associazioni, etc);
 - indicazione chiara dell'oggetto dell'istanza di accesso, in quanto sono inammissibili istanze generiche, che non consentano l'individuazione degli atti richiesti, istanze massive ed esplorative, volte ad un controllo generalizzato sull'operato della PA;
 - presenza della motivazione, dalla quale si evinca un interesse all'accesso che sia diretto, concreto, attuale e collegato alla documentazione richiesta;
- c) eventuale richiesta di integrazione dell'istanza, qualora dai controlli effettuati, la stessa risulti irregolare o incompleta. La richiesta di integrazione deve essere trasmessa al soggetto istante entro 10 giorni dalla ricezione della domanda di accesso agli atti, con l'indicazione che il procedimento si considera interrotto e il termine di 30 giorni ricomincerà a decorrere nuovamente dalla data di presentazione dell'istanza corretta o dell'integrazione richiesta;
- d) verifica della presenza di soggetti controinteressati, ossia di persone, individuate o facilmente individuabili dal tenore degli atti, che dall'esercizio dell'accesso documentale vedrebbero compromesso il loro diritto alla riservatezza;
- e) notifica agli eventuali controinteressati, i quali devono essere notiziati della ricezione dell'istanza di accesso agli atti da parte di ACSS e della facoltà di proporre una motivata opposizione all'accesso, entro 10 giorni dal ricevimento della comunicazione. Qualora per il numero dei destinatari la comunicazione personale non sia possibile o risulti particolarmente gravosa, il Responsabile, motivando adeguatamente, può disporre altre forme di pubblicità indiretta, quali comunicati stampa, avvisi pubblici o altri tipi di comunicazione pubblica che comunque diano garanzia di raggiungere i soggetti interessati dal provvedimento;

- f) verifica della ricezione della comunicazione da parte dei controinteressati e valutazione dell'eventuale opposizione all'accesso: l'opposizione non è vincolante ai fini dell'accoglimento o del rigetto della richiesta, ma ha lo scopo di fornire elementi utili per lo svolgimento di un'istruttoria imparziale e completa;
- g) redazione del provvedimento di accoglimento, differimento o diniego e trasmissione dello stesso all'istante, entro il termine procedimentale di 30 giorni.
Qualora le modalità per l'esercizio del diritto di accesso comportino il rimborso di eventuali diritti o spese a carico dell'Ente, il provvedimento recherà tale comunicazione e la documentazione potrà essere inviata successivamente alla verifica dell'avvenuto pagamento da parte del richiedente.

12. TERMINI PROCEDIMENTALI

1. Il procedimento di accesso deve concludersi nel termine di trenta giorni decorrenti dalla presentazione dell'istanza all'ufficio competente, ai sensi dell'art. 6 del D.P.R. n. 184/2006. L'art. 25 della L. n. 241/1990 prevede che, decorso inutilmente il termine, la richiesta si intende respinta.
2. Detto termine può essere elevato per il tempo strettamente necessario, nel caso in cui i soggetti controinteressati non siano di facile reperibilità. Il Responsabile del procedimento, in tali casi, provvede a comunicare all'interessato il differimento o la sospensione del termine, con apposita comunicazione motivata.

13. CONCLUSIONE DEL PROCEDIMENTO CON ACCOGLIMENTO DELLA RICHIESTA

1. Il Responsabile del procedimento decide sull'istanza di accesso con apposito atto, trasmesso al richiedente mediante mezzo idoneo ad accertarne la ricezione, ovvero all'indirizzo e-mail indicato espressamente dal richiedente.
Ove sussistano tutti i requisiti della domanda e non vi siano motivi per negare o differire il diritto d'accesso (cfr. artt. 14 e 15), la richiesta viene accolta, consentendo al soggetto interessato la visione dei documenti o la ricezione di copia degli stessi.
2. La documentazione è trasmessa preferibilmente in forma digitale. Nel caso in cui si dovesse procedere al riscontro mediante copia cartacea, al richiedente saranno imputati i costi di segreteria. Nel caso in cui sia necessaria copia autentica (in bollo) del documento, il derivante onere sarà posto in capo all'interessato.
3. L'accesso ai documenti può essere accolto limitatamente ad alcune parti, quando ricorre l'esigenza di differire o escludere l'accesso alle restanti parti, che vengono indicate tramite "omissis". Il Responsabile del procedimento provvede a rendere non intellegibili i dati personali non pertinenti e, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di accesso agli atti.
4. In ogni caso non è consentito utilizzare per fini non personali, riprodurre, diffondere o usare a fini commerciali le informazioni ottenute mediante l'esercizio del diritto di accesso documentale.

14. CONCLUSIONE DEL PROCEDIMENTO CON PROVVEDIMENTO DI DINIEGO

1. Il provvedimento di diniego deve essere motivato, con riferimento alla normativa vigente, alla individuazione delle categorie di cui all'art. 24 della L. n. 241/1990 e alle circostanze di fatto per cui la richiesta non può essere accolta così come proposta.

2. Il diritto di accesso deve essere negato laddove non si riscontri la sussistenza di un interesse personale, concreto, diretto ed attuale, per la tutela di situazioni giuridicamente rilevanti collegate agli atti richiesti.

3. Con riferimento ai casi di esclusione ai sensi dell'art. 24 della L. n. 241/1990 e dell'art. 10 del D.P.R. n. 184/2006, il diritto di accesso **deve** essere escluso:

- a) per i documenti coperti da segreto di Stato;
- b) per gli atti dei procedimenti tributari;
- c) per i documenti riguardanti l'attività dell'Agenzia diretta all'adozione di atti amministrativi generali, di pianificazione e di programmazione;
- d) per i documenti contenenti informazioni di carattere psico-attitudinale relative a terzi, nell'ambito di procedure selettive;
- e) nei casi di segreto e di divieto di divulgazione previsti dalla legge, tra cui:
 - il segreto istruttorio in sede penale (art. 329 c.p.p.);
 - il segreto investigativo in sede amministrativo-contabile (artt. 56, 57, 58 D.Lgs. n. 174/2016);
 - il segreto statistico (D.Lgs. n. 322/1989), il segreto tributario (D.P.R. n. 605/1983) e il segreto bancario (D.Lgs. n. 385/1993);
 - il segreto scientifico e industriale (art. 623 c.p.);
 - il segreto professionale, con applicazione anche agli atti difensivi, ai pareri legali e alla inerente corrispondenza, formati dai legali interni o esterni alla PA, in relazione a contenziosi in atto o potenziali.

4. Con riferimento ai casi in cui l'accesso **può** essere escluso, all'esito di un procedimento di valutazione e bilanciamento con l'interesse sotteso alla richiesta di accesso, si rilevano le seguenti casistiche, ai sensi dell'art. 24 c. 6 della L. n. 241/1990:

- a) quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini;
- b) quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono.

5. Con riferimento alle suddette categorie, sono individuati dall'Agenzia i seguenti documenti, il cui accesso può essere escluso, all'esito del procedimento di valutazione e bilanciamento degli interessi contrapposti:

- a) documenti contenenti informazioni su soggetti terzi relative alle condizioni psico-fisiche, economiche e sociali, opinioni politiche, convinzioni religiose, reputazione, uso di sostanze stupefacenti, procedimenti e condanne penali, corrispondenza personale, relazione e stati familiari, rapporti economici tra coniugi;
- b) atti riguardanti interventi di assistenza sociale o sussidi, indennizzi e contributi quando gli atti siano connessi allo stato di necessità degli interessati o quando dalla loro divulgazione possa comunque derivare pregiudizio al diritto alla riservatezza;
- c) documentazione inerente ai sinistri e alle richieste di risarcimento del danno;
- d) fascicoli personali dei dipendenti, atti o documenti attinenti ad inchieste ispettive, procedimenti e provvedimenti disciplinari;
- e) atti riguardanti il trattamento economico individuale in servizio e in quiescenza, quando dagli atti possano desumersi informazioni o notizie di carattere riservato, nonché documenti relativi ai pignoramenti sulle retribuzioni;
- f) atti contenenti denunce, segnalazioni ed esposti trasmessi alle autorità competenti in ordine a presunte violazioni di norme giuridiche, qualora non siano coperte da segreto istruttorio o investigativo;
- g) documenti oggetto di vertenze giudiziarie ed extragiudiziali o comunque inerenti alle stesse la cui divulgazione potrebbe compromettere l'esito del giudizio, o la cui diffusione potrebbe concretizzare violazione dell'obbligo del segreto;
- h) atti contenenti i risultati di indagini effettuate allo scopo di orientare l'attività di vigilanza ed ispezione ed i programmi operativi di intervento per tale attività;
- i) documentazione contenente dati di carattere industriale, commerciale o finanziario, la cui divulgazione possa provocare una lesione immediata e diretta degli interessi di un'impresa;
- j) atti che contengono informazioni tecniche, progetti, studi e realizzazioni dell'ingegno, tutelati da specifiche normative in materia di brevetto;
- k) ogni altro documento indicato dal prevalente indirizzo giurisprudenziale.

6. I documenti di cui ai punti 4 e 5 rimangono sempre accessibili da parte dei diretti interessati, dei loro legali rappresentanti, dei soggetti delegati, degli eredi legittimi e testamentari, fatta eccezione per il caso di documenti utili all'esperimento della strategia difensiva dell'Agenzia in sede giudiziaria, il cui accesso può essere differito sino all'esito del giudizio.

7. Per i soggetti terzi, titolari di un interesse qualificato, la disciplina dei casi di esclusione dell'accesso è temperata dal riconoscimento da parte dell'ordinamento del diritto di **accesso c.d. "difensivo"**: ai sensi del comma 7, art. 24, L. n. 241/1990, deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di **documenti contenenti dati sensibili e giudiziari**, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del D.Lgs. n. 196/2003 in caso di **dati idonei a rivelare lo stato di salute e la vita sessuale**. In presenza di questi ultimi, l'accesso può essere consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta

di accesso sia di rango almeno pari al diritto dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

8. L'accesso difensivo comporta un onere di allegazione particolarmente puntuale in capo all'istante e, in parallelo, un'approfondita valutazione da parte del Responsabile del procedimento che, nel bilanciamento degli interessi, può disporre modalità di accesso finalizzate a contemperare le opposte esigenze.

15. DIFFERIMENTO DEL DIRITTO DI ACCESSO

1. Il diritto di accesso agli atti non può essere negato ove sia sufficiente far ricorso al potere di differimento, ai sensi dell'art. 24 c. 4 della L. n. 241/1990.

2. Il differimento dell'accesso è disposto:

- per salvaguardare specifiche esigenze della P.A., specie nella fase istruttoria e preparatoria dei provvedimenti, in relazione a documenti la cui conoscenza possa compromettere il buon andamento dell'azione amministrativa;
- ove sia sufficiente assicurare una tutela temporanea agli interessi di cui all'art. 24, comma 6, della L. n. 241/90, con particolare riferimento alle esigenze di riservatezza relative a soggetti terzi o alla conduzione delle indagini relative ad uno specifico procedimento.

3. L'atto che dispone il differimento dell'accesso ne indica la motivazione e la durata, nei limiti strettamente necessari al rispetto delle finalità previste, ed è comunicato al richiedente entro i 30 giorni previsti per la conclusione del procedimento.

16. CONTROVERSIE RELATIVE ALL'ACCESSO

1. I provvedimenti di diniego o di differimento devono contenere l'indicazione dei termini e dell'Autorità presso la quale è possibile ricorrere. Nel caso in cui l'istanza non venga accolta e nel caso di diniego tacito, il richiedente può presentare ricorso, nel termine di trenta giorni, al Tribunale Amministrativo Regionale competente, ai sensi dell'art. 116 del D.Lgs. n. 104/2010, recante il Codice del Processo Amministrativo.

2. Nello stesso termine di 30 giorni, può essere presentata istanza di riesame della richiesta di accesso al Difensore Regionale della Lombardia, in applicazione dell'art. 16, lettera c, della L.R. Lombardia n. 1/2012 e dell'art. 13 della L.R. Lombardia n. 18/2010.

17. NORMATIVE SPECIALI IN MATERIA DI ACCESSO

1. L'accesso agli atti delle procedure di affidamento e di esecuzione dei contratti pubblici, non soggetti a pubblicazione obbligatoria sul sito istituzionale, è disciplinato dagli artt. 53 e 162 del D.Lgs. n. 50/2016

e dalle norme correlate, fatta salva l'applicabilità residuale della L. n. 241/1990, artt. 22 ss., per tutti gli aspetti non incompatibili.

2. L'accesso agli atti contenenti informazioni ambientali è disciplinato dagli artt. 3 e 5 del D.Lgs. n. 195 del 19/08/2005 "Attuazione della direttiva 2003/4/CE sull'accesso del pubblico all'informazione ambientale".

3. L'accesso alle segnalazioni dei pubblici dipendenti e dei lavoratori delle imprese che forniscono beni o servizi all'Agenzia c.d. "whistleblowing" è regolato dall'art. 54-bis del D.Lgs. n. 165/2001.

4. Il diritto di accesso dei Consiglieri regionali è disciplinato dall'art. 13, c. 5, della Legge Statutaria della Lombardia n. 1/2008 e dall'art. 112 del Regolamento generale del Consiglio regionale della Lombardia, n. 840 del 2009.

5. L'accesso agli atti ai fini delle indagini difensive in sede penale è disciplinato dall'art. 391-quater del Codice di Procedura Penale. In caso di diniego da parte dell'Ente, il difensore può rivolgere all'Ufficio del Pubblico Ministero un'apposita richiesta scritta, in applicazione degli artt. 367 e 368 c.p.p..

6. Il diritto di accesso ai propri dati personali è regolato dall'art. 15 del Regolamento generale sulla protezione dei dati (UE/2016/679) e non è soggetto agli stessi limiti posti dalla legge per l'accesso documentale.

SEZIONE III

DIRITTO DI ACCESSO CIVICO SEMPLICE

18. PRINCIPI E OGGETTO DELL'ACCESSO CIVICO SEMPLICE

1. L'Agenzia di Controllo del Sistema Sociosanitario lombardo, attraverso il proprio sito internet, garantisce l'accessibilità dei dati, delle informazioni e dei documenti che costituiscono obblighi di pubblicazione ai sensi della normativa sulla trasparenza, favorendo così forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.
2. Il diritto di accesso civico semplice, disciplinato dall'art. 5, c. 1, del D.Lgs. n. 33/2013, comporta il diritto di chiunque di richiedere i dati, le informazioni e i documenti la cui pubblicazione è obbligatoria ai sensi della normativa vigente e che l'amministrazione abbia omesso di pubblicare all'interno della sezione "Amministrazione Trasparente" del proprio sito internet istituzionale.

19. LEGITTIMAZIONE ALL'ACCESSO

1. L'esercizio del diritto di accesso civico semplice non è sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente: chiunque può esercitarlo, senza la necessità di essere titolare di un interesse qualificato o di indicare una motivazione. Il richiedente ha unicamente l'onere di indicare le proprie generalità, ivi compresi i propri recapiti, e di identificare chiaramente i dati, le informazioni o i documenti richiesti, di cui è stata omessa la pubblicazione obbligatoria.

20. MODALITÀ DI ESERCIZIO

1. Il diritto di accesso civico semplice si esercita indirizzando al Responsabile della Prevenzione della corruzione e della Trasparenza di ACSS un'apposita richiesta scritta, redatta preferibilmente sulla modulistica reperibile sul sito istituzionale dell'Agenzia (sezione "Amministrazione Trasparente" > "Accesso civico"), corredata dalla copia di un documento d'identità e trasmessa all'indirizzo PEC acss@pec.regione.lombardia.it o all'indirizzo mail responsabile.anticorruzione@acsslombardia.it.
2. Se l'istanza risulta generica o incompleta, il Responsabile della Prevenzione della corruzione e della Trasparenza ne dà comunicazione al richiedente, invitandolo a regolarizzarla ed informandolo che i termini del procedimento ricominceranno a decorrere dalla data di presentazione delle integrazioni richieste, necessarie ai fini della conclusione del procedimento.

21. ISTRUTTORIA E CONCLUSIONE DEL PROCEDIMENTO

1. Il Responsabile della Prevenzione della corruzione e della Trasparenza provvede a verificare i presupposti dell'istanza, in collaborazione con le Strutture competenti a formare i dati e documenti richiesti o a detenerli stabilmente. Le Strutture trasmettono al RPCT i dati eventualmente mancanti nella sezione "Amministrazione Trasparente" del sito web istituzionale, per la relativa pubblicazione.
2. Entro il termine di 30 giorni dal ricevimento dell'istanza, l'RPCT conclude il procedimento trasmettendo al richiedente i dati e i documenti richiesti o il link alla pagina web dove gli stessi sono pubblicati.

22. RICORSI

1. In caso di diniego, ritardo o mancata risposta entro i termini da parte del Responsabile della Prevenzione della corruzione e Trasparenza, il richiedente può ricorrere al titolare del potere sostitutivo di cui all'art. 2, c. 9-bis, della L. n. 241/1990, il quale conclude il procedimento di accesso civico semplice nel termine di 15 giorni.
2. A fronte del mancato accoglimento dell'istanza di accesso civico, il richiedente, ai fini della tutela del proprio diritto, può proporre ricorso al Tribunale Amministrativo Regionale (TAR) secondo quanto disposto dal Codice del Processo Amministrativo di cui al D.Lgs. n. 104/2010.

SEZIONE IV

DIRITTO DI ACCESSO CIVICO GENERALIZZATO

23. PRINCIPI E OGGETTO DEL DIRITTO DI ACCESSO CIVICO GENERALIZZATO

1. Il diritto di accesso civico generalizzato, di cui agli artt. 5 c. 2 e 5-bis del D.Lgs. n. 33/2013, ha lo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche, nonché di promuovere la partecipazione al dibattito pubblico.
2. L'accesso civico si esercita relativamente a documenti, informazioni e dati ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria sul sito istituzionale dell'Agenzia. Nell'ambito di tale tipologia di accesso, acquistano rilevanza non solo i documenti amministrativi, ma anche i dati e le informazioni detenuti dall'amministrazione, che non richiedano un lavoro di rielaborazione o di raccolta aggiuntivi rispetto a quelli svolti per i fini istituzionali.

24. SOGGETTI LEGITTIMATI

1. L'esercizio del diritto di accesso civico generalizzato non è sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente: chiunque può esercitarlo, senza la necessità di essere titolare di un interesse qualificato. L'indicazione della motivazione sottesa alla richiesta è facoltativa. Il richiedente ha unicamente l'onere di indicare le proprie generalità e di identificare chiaramente i dati, le informazioni o i documenti richiesti.
2. L'accesso civico generalizzato deve essere sempre garantito al richiedente nel rispetto dei limiti previsti dalla normativa, relativamente alla tutela di interessi giuridicamente rilevanti (art. 5-bis D.Lgs. n. 33/2013 e Linee Guida di cui alla deliberazione ANAC n. 1309 del 28.12.2016).

25. MODALITÀ DI ESERCIZIO

1. Il diritto di accesso civico generalizzato si esercita indirizzando all'Agenzia di Controllo del Sistema Sociosanitario lombardo un'apposita richiesta scritta, redatta preferibilmente sulla modulistica reperibile sul sito istituzionale dell'Agenzia (sezione "Amministrazione Trasparente" > "Altri contenuti" > "Accesso Civico"), unitamente a copia del documento di identità, da trasmettere via PEC all'indirizzo acss@pec.regione.lombardia.it, oppure tramite posta ordinaria o elettronica, agli indirizzi indicati sul sito istituzionale.

2. Le istanze ricevute vengono protocollate e assegnate in competenza alla Struttura che ha prodotto o detiene la documentazione richiesta, ed in conoscenza alla Struttura individuata dagli atti aziendali vigenti quale centro di competenza in materia di accesso agli atti.
3. Qualora la richiesta sia di competenza di un'altra Pubblica Amministrazione, l'Agenzia assiste il richiedente nella individuazione dell'amministrazione competente, a cui l'istanza va inviata nuovamente.
4. L'istanza deve identificare i dati, le informazioni o i documenti di cui si chiede l'accesso; non sono infatti ammesse richieste meramente esplorative o avanzate in modo generico. Ferma restando l'assenza dell'obbligo di motivazione, il richiedente può comunque indicare le finalità dell'accesso, in modo da agevolare il Responsabile del Procedimento nella valutazione della richiesta.
5. Al fine di agevolare le comunicazioni tra amministrazione e richiedente, quest'ultimo ha facoltà di indicare nell'istanza di accesso il proprio indirizzo e-mail quale recapito utilizzabile dall'Agenzia per l'invio delle successive comunicazioni.

26. ADEMPIMENTI ISTRUTTORI DEL RESPONSABILE DEL PROCEDIMENTO

1. Responsabile del procedimento di accesso civico generalizzato è il responsabile della Struttura che ha prodotto o detiene i dati, le informazioni e i documenti oggetto dell'istanza. Qualora la richiesta riguardi diversi dati, di competenza di più Strutture, il responsabile unico del procedimento di accesso civico generalizzato viene individuato dal RPCT.
2. Il Responsabile del procedimento, nel trattare la richiesta, può instaurare un "dialogo cooperativo" con il richiedente (cfr. circolare del Dipartimento della Funzione Pubblica n. 2/2017), e provvede ai seguenti adempimenti istruttori:
 - a) accertamento della propria competenza per materia, con riferimento ai dati e documenti richiesti;
 - b) verifica dell'identità del richiedente, appurando che sia stata allegata copia della carta d'identità;
 - c) valutazione dell'oggetto della domanda: i documenti, i dati o le informazioni richieste devono essere indicati in maniera chiara, in quanto non sono ammissibili istanze generiche o esplorative. Nel caso in cui vengano presentate una o più domande di accesso per un numero manifestamente irragionevole di documenti (istanze massive o seriali), è necessario ponderare il diritto all'accesso con il carico di lavoro che ne deriverebbe, al fine di salvaguardare il buon andamento dell'attività amministrativa;
 - d) richiesta di integrazione dell'istanza, qualora dai controlli effettuati, la stessa risulti irregolare o incompleta. Il Responsabile avvia un dialogo collaborativo con il richiedente, al fine di giungere ad un'adeguata definizione dell'oggetto della domanda. La richiesta di precisazioni deve essere inviata in maniera tempestiva e deve precedere necessariamente, ove non ottemperata, l'eventuale dichiarazione di inammissibilità dell'istanza, quale provvedimento conclusivo;
 - e) verifica dell'assenza di cause di esclusione e dei limiti all'accesso indicati dalla legge (art. 5-bis del D.Lgs. n. 33/2013), di cui ai successivi articoli 28 e 29 del presente regolamento;

- f) verifica dell'eventuale presenza di soggetti controinteressati, ossia di persone fisiche o giuridiche alle quali l'esercizio del diritto di accesso comporterebbe un pregiudizio concreto, con riferimento alla protezione dei dati personali, alla libertà e segretezza della corrispondenza ed alla tutela di interessi economici e commerciali, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali;
- g) notifica ai controinteressati, i quali devono essere notiziati della ricezione dell'istanza di accesso civico generalizzato da parte dell'Agenzia – da allegare in copia – e della facoltà di proporre una motivata opposizione entro 10 giorni dalla data in cui ricevono la comunicazione.
L'invio della notifica, tramite raccomandata a/r o per via telematica, per coloro che abbiano consentito tale forma di comunicazione, sospende i termini del procedimento, che ricominciano a decorrere dal momento in cui perviene l'opposizione, oppure trascorsi 10 giorni dalla ricezione delle notifiche da parte di tutti i soggetti controinteressati;
- h) valutazione dell'eventuale opposizione all'accesso: l'opposizione non è vincolante ai fini dell'accoglimento o del rigetto della richiesta, ma ha lo scopo di fornire elementi utili per lo svolgimento di un'istruttoria imparziale e completa;
- i) redazione del provvedimento di accoglimento, differimento o diniego e trasmissione dello stesso all'istante, con contestuale comunicazione ai soggetti controinteressati. Nel caso in cui la richiesta di accesso venga accolta nonostante l'opposizione di uno o più controinteressati, il provvedimento deve precisare che la trasmissione dei dati o dei documenti avverrà qualora, decorso 15 giorni dal ricevimento da parte dei controinteressati della comunicazione relativa all'accoglimento, non siano stati notificati all'Agenzia ricorsi o richieste di riesame sulla medesima domanda di accesso;
- j) trasmissione dei dati o della documentazione, secondo le modalità indicate nell'istanza di accesso, previa verifica del pagamento degli eventuali costi di riproduzione e spedizione e nel rispetto del termine di 15 giorni di cui al punto precedente, ai sensi dell'art. 5, c. 6, del D.Lgs. n. 33/2013.

27. TERMINI PROCEDIMENTALI

1. Il procedimento di accesso civico generalizzato deve concludersi con provvedimento espresso e motivato nel termine di trenta giorni dalla presentazione dell'istanza, fatti salvi i periodi di sospensione dei termini per le notifiche ai soggetti controinteressati. L'esito deve essere comunicato al richiedente e agli eventuali soggetti controinteressati.

2. Il Responsabile della Prevenzione della corruzione e della Trasparenza può chiedere in ogni momento al Responsabile del procedimento informazioni sull'esito delle istanze ricevute.

28. CAUSE TASSATIVE DI ESCLUSIONE DELL'ACCESSO

- 1. Il diritto di accesso civico generalizzato, ai sensi dell'art. 5, c. 3, del D.Lgs. n. 33/2013, è escluso:
 - a) nei casi di segreto di Stato (cfr. art. 39, legge n. 124/2007);

- b) nei casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'art. 24, c. 1, legge n. 241/1990:
 - atti dei procedimenti tributari, regolati da disciplina speciale;
 - nei confronti dell'attività dell'ente diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione;
 - nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi;
- c) nei casi di divieti di accesso o di divulgazione previsti dalla legge, tra cui, a titolo esemplificativo:
 - il segreto militare (R.D. n. 161/1941);
 - il segreto statistico (D.Lgs. n. 322/1989) e il segreto bancario (D.Lgs. n. 385/1993);
 - il segreto scientifico e il segreto industriale (art. 623 c.p.);
 - il segreto istruttorio penale (art. 329 c.p.p.);
 - il segreto sul contenuto della corrispondenza (art. 616 c.p.);
 - i divieti di divulgazione connessi al segreto d'ufficio (art. 15, D.P.R. n. 3/1957);
 - il divieto di diffusione dei dati idonei a rivelare lo stato di salute e la vita sessuale (art. 7-bis, c. 6, D.Lgs. n. 33/2013);
 - il divieto pubblicazione, e conseguentemente di divulgazione generalizzata, dei dati identificativi di persone fisiche beneficiarie di aiuti economici da cui è possibile ricavare informazioni relative allo stato di salute ovvero alla situazione di disagio economico-sociale (art. 26, c. 4, D.Lgs. n. 33/2013).

2. Le cause di esclusione dell'accesso di cui al presente articolo hanno carattere tassativo: il Responsabile del procedimento è quindi tenuto a negare l'accesso, trattandosi di eccezioni poste da una norma di rango primario, sulla base di una valutazione preventiva e generale, a tutela di interessi pubblici e privati fondamentali e prioritari rispetto a quello del diritto alla conoscenza diffusa.

29. LIMITI RELATIVI ALL'ESERCIZIO DEL DIRITTO DI ACCESSO CIVICO GENERALIZZATO

1. I "limiti relativi" all'accesso generalizzato sono posti dal legislatore a tutela di interessi pubblici e privati di particolare rilievo giuridico, che l'Agenzia deve necessariamente valutare con la tecnica del bilanciamento, caso per caso, tra l'interesse pubblico alla divulgazione generalizzata e la tutela di altrettanto validi interessi considerati dall'ordinamento.

2. La disciplina dell'accesso civico generalizzato, in particolare, prevede la possibilità di rigettare l'istanza qualora il diniego sia necessario per evitare un pregiudizio concreto alla tutela di uno degli interessi pubblici elencati nell'art. 5-bis, comma 1, del D.Lgs. n. 33/2013, inerenti:

- a) la sicurezza pubblica e l'ordine pubblico;
- b) la sicurezza nazionale;
- c) la difesa e le questioni militari;
- d) le relazioni internazionali;
- e) la politica e la stabilità finanziaria ed economica dello Stato;

- f) la conduzione di indagini sui reati e il loro perseguimento - in particolare, possono essere sottratti all'accesso, ove sia rilevata la sussistenza del pregiudizio concreto:
- gli atti, i documenti e le informazioni concernenti azioni di responsabilità penale e contabile, rapporti e denunce trasmesse all'Autorità giudiziaria (al di fuori dei casi di segreto istruttorio e investigativo) o comunque atti riguardanti controversie pendenti, nonché i certificati penali;
 - i rapporti con la Procura della Repubblica e con la Procura regionale della Corte dei Conti e richieste o relazioni di dette Procure, ove siano nominativamente individuati i soggetti per i quali si manifesta la sussistenza di responsabilità amministrative, contabili o penali;
- g) il regolare svolgimento di attività ispettive - le limitazioni all'accesso, soprattutto nella fase endoprocedimentale ispettiva, possono essere motivate dall'evitare il pregiudizio al regolare svolgimento della stessa e possono riguardare a mero titolo di esempio le notizie sulla programmazione dell'attività di vigilanza, sulle modalità e i tempi del suo svolgimento, le indagini sull'attività degli uffici, dei singoli dipendenti, o sull'attività di enti pubblici e privati su cui l'amministrazione esercita forme di vigilanza. Ciò vale sia per le richieste e le indagini condotte d'ufficio, sia per quelle avviate su segnalazione di privati, di organizzazioni di categoria o sindacali e similari.

3. Il D.Lgs. n. 33/2013 ha previsto inoltre, all'art. 5-bis, comma 2, che l'accesso generalizzato possa essere rifiutato nei casi in cui il diniego sia necessario per evitare un pregiudizio concreto alla tutela degli interessi privati specificamente indicati dalla norma, relativi a soggetti controinteressati:

- a) protezione dei dati personali - in conformità con la disciplina legislativa vigente in materia;
- b) libertà e segretezza della corrispondenza - in tal caso l'Agenzia dovrà tenere in considerazione la natura della corrispondenza, le intenzioni dei soggetti coinvolti e la legittima aspettativa di confidenzialità degli interessati. Il limite all'accesso quindi non riguarda necessariamente tutte le comunicazioni, ma soltanto quelle che, secondo una verifica da operare caso per caso, abbiano effettivamente un carattere confidenziale e privato;
- c) interessi economici e commerciali di una persona fisica o giuridica - ivi compresi proprietà intellettuale, diritto d'autore e segreti commerciali, ambiti specifici tutelati dall'ordinamento e collegati con l'interesse generale di garanzia del buon funzionamento delle regole del mercato e della libera concorrenza.

4. I casi di limitazione dell'accesso per la tutela degli interessi pubblici e privati sopra elencati devono essere interpretati alla luce delle indicazioni operative fornite dall'ANAC nella deliberazione n. 1309/2016 ed eventuali successive integrazioni.

5. In particolare, ai fini della valutazione del pregiudizio concreto arrecabile ad interessi privati, vanno prese in considerazione le conseguenze – anche legate alla sfera morale, relazionale e sociale – che potrebbero derivare ai controinteressati dalla conoscibilità, da parte di chiunque, del dato o del documento richiesto. L'art. 3 c. 1 del D.Lgs. n. 33/2013, infatti, prevede che i dati e i documenti forniti al richiedente tramite l'accesso generalizzato siano considerati come «pubblici», sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 7 del D.Lgs. n. 33/2013).

6. In applicazione del principio di proporzionalità, secondo il quale le deroghe non devono eccedere quanto è adeguato per il raggiungimento dello scopo perseguito, qualora i limiti di cui al presente

articolo riguardino soltanto alcuni dati o alcune parti dei documenti richiesti, deve essere consentito un accesso parziale, utilizzando, se del caso, la tecnica dell'oscuramento ("omissis").

7. L'accesso generalizzato, infine, non può essere negato ove sia sufficiente fare ricorso al potere di differimento, per un periodo determinato ed indicato nel provvedimento, al fine di tutelare gli interessi giuridicamente rilevanti individuati nel caso concreto.

30. ACCOGLIMENTO DELLA RICHIESTA DI ACCESSO GENERALIZZATO

1. L'accoglimento della richiesta viene comunicata al richiedente e ai controinteressati mediante mezzo idoneo ad accertarne la ricezione, oppure all'indirizzo e-mail espressamente indicato.

2. Nel caso in cui la richiesta di accesso sia stata accolta nonostante l'opposizione del soggetto controinteressato, il provvedimento deve essere motivato circa l'insussistenza di pregiudizi concreti agli interessi privati e deve precisare che i dati o i documenti richiesti non possono essere trasmessi al richiedente prima di quindici giorni dalla ricezione dell'esito del procedimento da parte del controinteressato che si è opposto. L'Agenzia può trasmettere immediatamente i documenti, disapplicando tale termine, esclusivamente nei casi di comprovata indifferibilità dell'accesso.

3. Il rilascio di dati o documenti in formato elettronico, in risposta alla richiesta di accesso civico generalizzato, è gratuito. Nel caso in cui venga richiesta copia cartacea, al richiedente potranno essere imputate le relative spese. Nel caso in cui sia necessaria copia autentica (in bollo) del documento, il derivante onere sarà posto in capo all'interessato.

31. DINIEGO, LIMITAZIONE E DIFFERIMENTO

1. L'Agenzia deve motivare l'eventuale rifiuto, differimento o limitazione dell'accesso civico generalizzato con riferimento ai soli casi e limiti stabiliti dall'art. 5-bis del D.Lgs. n. 33/2013, di cui agli articoli 28 e 29 del presente regolamento.

2. Il Responsabile del procedimento, nel provvedimento conclusivo, deve indicare i mezzi di riesame e di ricorso esperibili ai sensi di legge.

32. RIESAME DEI PROVVEDIMENTI ADOTTATI

1. Il richiedente, nei casi di diniego totale o parziale dell'accesso civico o di mancata risposta entro il termine, ovvero i soggetti controinteressati, nei casi di accoglimento della richiesta di accesso, possono presentare richiesta di riesame al Responsabile della prevenzione della corruzione e della trasparenza (RPCT), che decide con provvedimento motivato, entro il termine di venti giorni decorrenti dalla presentazione della domanda di riesame.

2. Se l'accesso generalizzato è stato negato o differito a tutela della protezione di dati personali, in conformità alla disciplina legislativa vigente in materia, il Responsabile della Prevenzione della corruzione e della Trasparenza provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del RPCT è sospeso, fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni.

3. Nel caso in cui i documenti o i dati richiesti siano detenuti dallo stesso Responsabile della Prevenzione della corruzione e della Trasparenza, la competenza a decidere sulle istanze di riesame è in capo alla Direzione Generale.

33. RICORSI

1. Il richiedente l'accesso civico generalizzato o i soggetti controinteressati all'accesso possono presentare ricorso avverso ai provvedimenti assunti dal Responsabile del procedimento o, in caso di riesame, dal Responsabile della Prevenzione della corruzione e della Trasparenza, avanti al difensore civico competente per ambito territoriale. Il termine per proporre opposizione avanti al TAR decorre dalla data di ricezione, da parte del richiedente, del provvedimento del Difensore Regionale.

2. Avverso le decisioni dell'Agenzia sulle istanze di accesso civico, avverso il silenzio inadempienza formatosi per il mancato rispetto dei termini, o avverso la decisione del Responsabile della Prevenzione della corruzione e della Trasparenza sull'istanza di riesame, il richiedente o il controinteressato possono proporre ricorso al Tribunale amministrativo regionale territorialmente competente.

SEZIONE V

NORME FINALI

34. NORME DI RINVIO ED ENTRATA IN VIGORE

1. Per quanto non espressamente disciplinato dal presente Regolamento, in materia di accesso documentale si applicano le disposizioni della L. n. 241/1990 e del D.P.R. n. 184/2006, in materia di accesso civico semplice e accesso civico generalizzato si applicano le disposizioni del D.Lgs. n. 33/2013, nonché le Linee Guida in materia redatte dall'Autorità Nazionale Anticorruzione (ANAC) e le Circolari del Ministero per la Semplificazione e la Pubblica Amministrazione.
2. Il presente Regolamento entra in vigore dalla data di adozione del relativo provvedimento di approvazione.

35. MODULISTICA

1. La modulistica utilizzabile dai soggetti interessati a presentare istanza di accesso documentale, accesso civico e accesso civico generalizzato viene pubblicata sul sito istituzionale dell'Agenzia e periodicamente aggiornata.



Regolamento per la Politica della Sicurezza delle Informazioni e la Cyber Security di ACSS

Approvato con:	Deliberazione del Comitato di Direzione
N.:	
Data:	
Versione:	1.0
Referente:	Alberto Panese

Agenzia di Controllo del Sistema Sociosanitario Lombardo
Sede Legale: Via Pola, 12 20124 Milano Tel. 02/8282.9800 - Fax 02/8282.9805
acss@pec.regione.lombardia.it
C.F. 97743230159

Sommario

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI	10
1. INTRODUZIONE	11
ART 1) SCOPO DEL DOCUMENTO	11
ART 2) CAMPO DI APPLICAZIONE	11
ART 3) DEFINIZIONI E ACRONIMI	12
2. OBIETTIVI DI SICUREZZA	13
ART 4) OBIETTIVI PER LA SICUREZZA DELLE INFORMAZIONI	13
3. ORGANIZZAZIONE E RESPONSABILITÀ	15
ART 5) ORGANIZZAZIONE E RESPONSABILITÀ PER LA SICUREZZA DELLE INFORMAZIONI	15
4. VALUTAZIONE DEI RISCHI	15
ART 6) SCENARI DI MINACCIA	15
5. RISCHI LEGATI ALLA CYBERSECURITY	16
ART 7) PRINCIPI GENERALI	16
ART 8) PROCESSO	17
ART 9) RISCHIO TOLLERATO	18
6. RISCHI LEGATI ALLA SUPPLY CHAIN	18
ART 10) PROCESSI DI GESTIONE DEL RISCHIO INERENTI ALLA CATENA DI APPROVVIGIONAMENTO CYBER	18
7. CONTROLLI DI SICUREZZA	19
ART 11) CONTROLLI DI SICUREZZA DELLE INFORMAZIONI	19
8. SICUREZZA DELLE RISORSE INFORMATIVE	19
ART 12) RISORSE INFORMATIVE	19
ART 13) INVENTARIO DEGLI ASSET	19
ART 14) UTILIZZO DEGLI ASSET	20
ART 15) CLASSIFICAZIONE E TRATTAMENTO DELLE INFORMAZIONI	22
ART 16) ASSEGNAZIONE DI PRIORITÀ AGLI ASSET	22
ART 17) UTILIZZO DI SUPPORTI E DISPOSITIVI INFORMATICI DELLA ACSS PER LA MEMORIZZAZIONE	23
ART 18) UTILIZZO DI SUPPORTI E DISPOSITIVI PERSONALI	23
ART 19) LAVORO DA REMOTO	23

9.	SICUREZZA NELL'AMBITO DELLE RISORSE UMANE.....	24
	ART 20) INDIVIDUAZIONE DEL PERSONALE.....	24
	ART 21) RESPONSABILITÀ DEL PERSONALE E DEI COLLABORATORI ESTERNI	24
	ART 22) SENSIBILIZZAZIONE E FORMAZIONE	24
	ART 23) CESSAZIONE E VARIAZIONE DEL RAPPORTO DI LAVORO.....	25
10.	SICUREZZA NELLE RELAZIONI CON I SOGGETTI TERZI.....	25
	ART 24) CONTROLLI GENERALI	25
	ART 25) CLAUSOLE CONTRATTUALI	26
	ART 26) MONITORAGGIO, REVISIONE E GESTIONE DEL CAMBIAMENTO DEI SERVIZI DELLE TERZE PARTI	26
	ART 27) SICUREZZA DELLE INFORMAZIONI PER L'UTILIZZO DEI SERVIZI CLOUD.....	26
11.	SICUREZZA FISICA E AMBIENTALE	27
	ART 28) PROTEZIONE DA MINACCE DI TIPO FISICO ED AMBIENTALE	27
	ART 29) SICUREZZA DELLE AREE	27
	ART 30) CONTROLLO DEGLI ACCESSI FISICI	27
	ART 31) SICUREZZA DEGLI UFFICI, DELLE STANZE E DEGLI STRUMENTI DI LAVORO	28
	ART 32) LAVORARE IN AREE SENSIBILI.....	28
	ART 33) Sicurezza delle aree di carico e scarico	28
	ART 34) EQUIPAGGIAMENTO DI SICUREZZA	28
	ART 35) SICUREZZA DEL CABLAGGIO.....	29
12.	SICUREZZA DELLE ATTIVITÀ OPERATIVE.....	29
	ART 36) PROCEDURE OPERATIVE E RESPONSABILITÀ.....	29
	ART 37) PROTEZIONE DA MALICIOUS SOFTWARE	29
	ART 38) SOFTWARE NON AUTORIZZATO	30
	ART 39) BACK-UP	30
	ART 40) SICUREZZA DELLA RETE DATI	31
	ART 41) SICUREZZA NELLO SCAMBIO DI INFORMAZIONI.....	31
	ART 42) MONITORAGGIO	32
	ART 43) CRITTOGRAFIA	33
	ART 44) SMALTIMENTO E CANCELLAZIONE SICURA DEI DATI.....	33
13.	CONTROLLO DEGLI ACCESSI	34
	ART 45) ACCESSO ALLE INFORMAZIONI E ALLE RISORSE ICT	34
	ART 46) REVISIONE DEI DIRITTI DI ACCESSO	34
14.	ACCESSI LOGICI.....	35
	ART 47) GESTIONE DELLE CREDENZIALI DI ACCESSO	35
	ART 48) GESTIONE DEI DIRITTI DI ACCESSO	35

ART 49) RESPONSABILITÀ DELL'UTENTE	36
ART 50) ACCESSO ALLA RETE E RELATIVI SERVIZI	36
ART 51) ACCESSI AL SISTEMA OPERATIVO ED AL SOFTWARE DI BASE	37
ART 52) ACCESSI AI SISTEMI ED ALLE APPLICAZIONI.....	37
15. ACQUISIZIONE, SVILUPPO E MANUTENZIONE	39
ART 53) ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI	39
ART 54) REQUISITI DI SICUREZZA DEI SISTEMI INFORMATIVI	39
ART 55) SICUREZZA NEI PROCESSI DI SVILUPPO E SUPPORTO	39
ART 56) SICUREZZA NELLA MANUTENZIONE	40
16. GESTIONE DEGLI INCIDENTI RILEVANTI AI FINI DELLA SICUREZZA	41
ART 57) GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI E DEI MIGLIORAMENTI.....	41
17. GESTIONE DELLA CONTINUITÀ OPERATIVA.....	42
ART 58) ASPETTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI NELLA GESTIONE DELLA CONTINUITÀ OPERATIVA.....	42
18. CONTROLLI DI CONFORMITÀ	42
ART 59) Conformità ai requisiti di sicurezza	42
19. CONFORMITÀ AI REQUISITI COGENTI E CONTRATTUALI	42
ART 60) NORMATIVA GENERALE IN MATERIA DI SICUREZZA DELLE INFORMAZIONI	42
ART 61) NORMATIVA SPECIFICA E DI SETTORE APPLICABILE AI SERVIZI DELLA ACSS.....	43
ART 62) REQUISITI CONTRATTUALI	43
20. CONFORMITÀ A STANDARD INTERNAZIONALI E BEST PRACTICES	43
ART 63) STANDARD INTERNAZIONALI E BEST PRACTICE.....	43
21. RIESAME DELLA SICUREZZA DELLE INFORMAZIONI	44
ART 64) VERIFICA E RIESAME DELLA SICUREZZA DELLE INFORMAZIONI	44
22. IL SISTEMA DOCUMENTALE	44
ART 65) SISTEMA DOCUMENTALE PER LA SICUREZZA DELLE INFORMAZIONI.....	44
23. DOCUMENTI DI RIFERIMENTO	45
RUOLI E RESPONSABILITÀ PER LA SICUREZZA DELLE INFORMAZIONI.....	48
1. INTRODUZIONE	48
ART 1) SCOPO DEL DOCUMENTO	48
ART 2) CAMPO DI APPLICAZIONE	48
ART 3) DEFINIZIONI E ACRONIMI.....	48

2.	RUOLI COINVOLTI NELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI.....	49
ART 4)	DIRETTORE GENERALE DELLA ACSS.....	49
ART 5)	COMITATO DIRETTIVO PER LA SICUREZZA DELLE INFORMAZIONI (CDSI)	49
ART 6)	RESPONSABILE DELLE RISORSE UMANE PER LA SICUREZZA DELLE INFORMAZIONI 50	
ART 7)	RESPONSABILE DEGLI APPROVVIGIONAMENTI PER LA SICUREZZA DELLE INFORMAZIONI	51
ART 8)	RESPONSABILE DELLA SICUREZZA DELLE INFORMAZIONI	51
ART 9)	RESPONSABILE DELLA SAFETY E DELLA SICUREZZA FISICA.....	52
ART 10)	RESPONSABILE DELLE FACILITIES	53
ART 11)	RESPONSABILE ICT.....	53
ART 12)	RESPONSABILE TECNOLOGIE BIOMEDICHE	54
ART 13)	REFERENTE NIS	54
ART 14)	VICARIO NIS	55
ART 15)	RESPONSABILE DI DIREZIONE SANITARIA, SOCIO-SANITARIA E AMMINISTRATIVA 55	
ART 16)	RESPONSABILE DI STRUTTURA/UFFICIO	55
ART 17)	PERSONALE DIPENDENTE O ASSIMILABILE.....	57
ART 18)	SOGGETTI TERZI.....	57
3.	FUNZIONI AZIENDALI COINVOLTE NELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI.....	57
ART 19)	CORRISPONDENZA TRA RUOLI COINVOLTI NELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI E FUNZIONI DELLA ACSS	57
4.	DOCUMENTI DI RIFERIMENTO	58
	LINEA GUIDA CONTINUITÀ OPERATIVA.....	59
1.	INTRODUZIONE	59
ART 1)	SCOPO	59
ART 2)	CAMPO DI APPLICAZIONE	59
ART 3)	DEFINIZIONI.....	59
ART 4)	ACRONIMI	61
ART 5)	CONTINUITÀ OPERATIVA	61
ART 6)	IL MODELLO PER IL SISTEMA DI BCM	62
1.1.1	FASE 1: DEFINIZIONE	63
1.1.1.1	AMBITO DEL SISTEMA DI BCM.....	64
1.1.1.2	POLITICA PER LA CONTINUITÀ OPERATIVA.....	64
1.1.1.3	ORGANIZZAZIONE, RUOLI E RESPONSABILITÀ DEL SISTEMA DI BCM.....	64
1.1.2	FASE 2: ASSESSMENT	65

1.1.2.1	RISK ASSESSMENT e RISK TREATMENT	66
1.1.3	FASE 3: PIANIFICAZIONE	67
1.1.3.1	DEFINIZIONE DELLA STRATEGIA DI CONTINUITÀ OPERATIVA	67
1.1.3.2	ANALISI DI FATTIBILITÀ E PROGETTAZIONE SOLUZIONE TECNICA/ORGANIZZATIVA	68
1.1.3.3	ANALISI DI FATTIBILITÀ TECNICA	68
1.1.3.4	PROGETTAZIONE SOLUZIONE TECNICA-ORGANIZZATIVA.....	68
1.1.3.5	PIANO DI CONTINUITÀ OPERATIVA/DISASTER RECOVERY (PCO/PDR)	69
1.1.3.6	PIANO DI ATTUAZIONE	70
1.1.4	FASE 4: ATTUAZIONE	70
1.1.4.1	REALIZZAZIONE DELLA SOLUZIONE TECNICO/ORGANIZZATIVA DEFINITA....	70
1.1.4.2	COMUNICAZIONE E FORMAZIONE	70
1.1.4.3	TEST E RELATIVE MODALITÀ.....	71
1.1.5	FASE 5: REVISIONE	71
1.1.5.1	TEST ED ESERCITAZIONI DI CO/DR	71
1.1.5.2	VALUTAZIONE DELLE PERFORMANCE DEL SISTEMA DI BCM	72
1.1.5.3	VERIFICHE INTERNE.....	72
1.1.5.4	MANTENIMENTO DEL PIANO DI CO/DR.....	73
1.1.5.5	RIESAME DELLA DIREZIONE	73
1.1.5.6	MIGLIORAMENTO CONTINUO.....	74
2.	DOCUMENTI DI RIFERIMENTO	75
POLITICA SPECIFICA PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA ICT		76
1.	INTRODUZIONE	76
ART 1)	SCOPO DEL DOCUMENTO	76
ART 2)	CAMPO DI APPLICAZIONE	76
ART 3)	DEFINIZIONI E ACRONIMI.....	76
2.	OBIETTIVI	79
ART 4)	OBIETTIVI DI SICUREZZA PER LA GESTIONE INCIDENTI DI SICUREZZA ICT.....	79
3.	GENERALITÀ.....	79
ART 5)	PROCESSO DI GESTIONE DEGLI INCIDENTI ICT	79
ART 6)	ORGANIZZAZIONE.....	80
ART 7)	TECNOLOGIE A SUPPORTO	80
4.	RILEVAZIONE DEGLI EVENTI DI SICUREZZA ICT	81
ART 8)	MONITORAGGIO DEGLI EVENTI DI SICUREZZA ICT.....	81
ART 9)	PRE-ANALISI DEGLI EVENTI DI SICUREZZA ICT.....	82
ART 10)	TRACCIAMENTO DEGLI EVENTI DI SICUREZZA ICT	83

5.	CLASSIFICAZIONE DEGLI EVENTI DI SICUREZZA ICT	84
	ART 11) GENERALITÀ	84
6.	CRITICITÀ DELL'EVENTO	85
	ART 12) VALUTAZIONE DELLA CRITICITÀ DELL'EVENTO DI SICUREZZA ICT	85
7.	TIPOLOGIA DELL'EVENTO	86
	ART 13) VALUTAZIONE DELLA TIPOLOGIA DELL'EVENTO DI SICUREZZA ICT	86
8.	PRIORITÀ DELL'EVENTO	88
	ART 14) DEFINIZIONE DEI LIVELLI DI PRIORITÀ	88
9.	AVVIO ATTIVITÀ DI TRATTAMENTO.....	88
	ART 15) AGGIORNAMENTO DELLA SCHEDA EVENTO	88
10.	GESTIONE DEGLI EVENTI DI SICUREZZA ICT	89
	ART 16) TRATTAMENTO DEGLI ALLARMI DI SICUREZZA ICT	89
	ART 17) TRATTAMENTO DEGLI INCIDENTI DI SICUREZZA ICT	90
11.	ANALISI POST-INCIDENTE DI SICUREZZA ICT	92
	ART 18) ANALISI POST-INCIDENTE DI SICUREZZA ICT	92
12.	MIGLIORAMENTO CONTINUO	93
	ART 19) MIGLIORAMENTO CONTINUO DEL PROCESSO DI GESTIONE INCIDENTI.....	93
13.	DOCUMENTI DI RIFERIMENTO	93
POLITICA SPECIFICA PER GLI AMMINISTRATORI DI SISTEMA		95
1.	INTRODUZIONE	95
	ART 1) SCOPO DEL DOCUMENTO	95
	ART 2) CAMPO DI APPLICAZIONE	96
	ART 3) DEFINIZIONI E ACRONIMI	96
2.	ETICA E COMPORTAMENTI SANZIONATI DALLE NORMATIVE VIGENTI	97
	ART 4) ETICA E COMPORTAMENTI SANZIONABILI	97
3.	RUOLO DI AMMINISTRATORE DI SISTEMA	98
	ART 5) DESCRIZIONE	98
4.	GESTIONE DEGLI AMMINISTRATORI DI SISTEMA	99
	ART 6) REQUISITI GENERALI.....	99
	ART 7) REQUISITI PER LA VALUTAZIONE DELLE CARATTERISTICHE SOGGETTIVE.....	100
	ART 8) REQUISITI PER LA DESIGNAZIONE INDIVIDUALE	100

ART 9) REQUISITI PER LA GESTIONE DELL'ELENCO DEGLI AMMINISTRATORI DI SISTEMA	101
ART 10) REQUISITI PER LA REGISTRAZIONE DEGLI ACCESSI	102
ART 11) REQUISITI PER LA VERIFICA DELLE ATTIVITÀ	103
ART 12) REQUISITI CONTRATTUALI PER LA GESTIONE DEI SERVIZI DI AMMINISTRAZIONE DI SISTEMA DA PARTE DI SOGGETTI TERZI (OUTSOURCING)	104
5. DOCUMENTI DI RIFERIMENTO	104
POLITICA SPECIFICA PER LA GESTIONE DELLE UTENZE	105
1. INTRODUZIONE	105
ART 13) SCOPO DEL DOCUMENTO	105
ART 14) CAMPO DI APPLICAZIONE	105
ART 15) DEFINIZIONI E ACRONIMI	105
2. ETICA E COMPORTAMENTI SANZIONATI DALLE NORMATIVE VIGENTI	107
ART 16) ETICA E COMPORTAMENTI SANZIONABILI	107
3. ACCESSO ALLE RISORSE INFORMATICHE	107
ART 17) REGOLE GENERALI	107
4. GESTIONE DELLE CREDENZIALI DI ACCESSO	108
ART 18) REGOLE GENERALI	108
5. GENERAZIONE DELLE CREDENZIALI DI ACCESSO	110
ART 19) GENERAZIONE DELLE CREDENZIALI	110
6. USERID POLICY	110
ART 20) PRINCIPI GENERALI	110
7. PASSWORD POLICY	110
ART 21) PRINCIPI GENERALI	110
ART 22) REGOLE SEMANTICHE PER LA COMPOSIZIONE DELLA PASSWORD	110
ART 23) REGOLE PER LA GESTIONE DEL CICLO DI VITA DELLE PASSWORD	111
ART 24) GENERAZIONE DELLE PASSWORD	111
ART 25) CUSTODIA DELLE PASSWORD	112
ART 26) SCADENZA DELLE PASSWORD	112
ART 27) MODIFICA DELLE PASSWORD	113
8. GESTIONE DEI PROFILI AUTORIZZATIVI	113
ART 28) PRINCIPI GENERALI	113
9. REGISTRAZIONE DELLE USERID AUTORIZZATE	114

ART 29) PRINCIPI GENERALI	114
10. DISATTIVAZIONE E BLOCCO DELLE CREDENZIALI	114
ART 30) DISATTIVAZIONE DELLE CREDENZIALI DI ACCESSO	114
ART 31) BLOCCO DELLE CREDENZIALI DI ACCESSO	115
11. VERIFICA PERIODICA DELLE CREDENZIALI E DELLE AUTORIZZAZIONI	115
ART 32) PRINCIPI GENERALI	115
12. DOCUMENTI DI RIFERIMENTO	115
POLITICHE PER LA CANCELLAZIONE SICURA E LO SMALTIMENTO DEI SUPPORTI ELETTRONICI	
117	
1. INTRODUZIONE	117
ART 1) SCOPO DEL DOCUMENTO	117
ART 2) CAMPO DI APPLICAZIONE	118
ART 3) DEFINIZIONI E ACRONIMI	118
2. REQUISITI GENERALI	119
3. CANCELLAZIONE E DISTRUZIONE SICURA DI INFORMAZIONI SU DISPOSITIVI	
ELETTRONICI O INFORMATICI	120
ART 4) MISURE PER IL REIMPIEGO/RICICLAGGIO E LO SMALTIMENTO DI RIFIUTI ELETTRICI	
ED ELETTRONICI	120
ART 5) REIMPIEGO SICURO DI DISPOSITIVI ELETTRONICI O INFORMATICI	120
ART 6) SMALTIMENTO SICURO DI RIFIUTI ELETTRICI ED ELETTRONICI	121
4. DISTRUZIONE SICURA DI INFORMAZIONI SU SUPPORTO CARTACEO	121
ART 7) DISTRUZIONE DI INFORMAZIONI SU SUPPORTO CARTACEO	121
5. RISPETTO DELL'AMBIENTE E CONTENIMENTO DEI COSTI	122
6. REQUISITI SPECIFICI IN CASO DI AFFIDAMENTO DEL SERVIZIO A SOGGETTI TERZI ...	122
ART 8) DEFINIZIONE DI ACCORDI CONTRATTUALI	122
ART 9) PRESA IN CONSEGNA/RITIRO DEL MATERIALE	124
ART 10) CANCELLAZIONE E DISTRUZIONE SICURA	124
7. DOCUMENTI DI RIFERIMENTO	125

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La mission dell'Agenzia di Controllo del Sistema Sociosanitario lombardo (di seguito ACSS) è quella di promuovere lo sviluppo e il consolidamento di un sistema di monitoraggio improntato al rafforzamento dei controlli in ambito sociosanitario, a garanzia dell'equità di accesso ai servizi e a tutela del rispetto dei principi di efficienza, efficacia, qualità, appropriatezza ed economicità delle prestazioni e dei servizi erogati.

La ACSS evidenzia eventuali comportamenti anomali e/o opportunismi e indirizza l'attività di controllo esercitata dalle ATS secondo una logica di miglioramento continuo della qualità del servizio, a garanzia dei cittadini e del rispetto dei Livelli Essenziali di Assistenza (LEA).

La ACSS, in linea con gli assi strategici e le priorità trasversali individuate nel Piano Nazionale di Ripresa e Resilienza (PNRR), ritiene che la digitalizzazione rappresenti un fattore determinante di governo e controllo. D'altra parte, l'utilizzo pervasivo delle tecnologie dell'informazione e della comunicazione implica l'esposizione degli Enti Sanitari a rischi cyber che devono essere opportunamente gestiti attraverso l'adozione di misure volte a conseguire un livello elevato di sicurezza della rete e dei sistemi informativi nonché una opportuna consapevolezza da parte di tutti gli operatori.

A tal fine, la ACSS adotta un approccio sistematico alla cybersecurity e più in generale alla sicurezza delle informazioni che indirizza un insieme organico e strutturato di misure di sicurezza logica, fisica, organizzativa e procedurale dedicate alla protezione dell'integrità, della riservatezza e della disponibilità delle informazioni e delle reti di comunicazione. L'implementazione di misure di sicurezza adeguate ed efficaci è, quindi, necessaria per garantire anche la sicurezza e la protezione dei dati personali contenuti all'interno del patrimonio informativo dell'ACSS. L'approccio alla cybersecurity è, dunque, coerente con il modello organizzativo definito dalla ACSS per assicurare la piena liceità e correttezza nei trattamenti dei dati personali effettuati.

In linea con tale approccio, la presente Politica declina un insieme di regole di base che indirizzano le strategie e le modalità di gestione della sicurezza delle informazioni della ACSS, stabilendo:

- gli obiettivi di sicurezza;
- l'ambito di applicazione e i destinatari della Politica di Sicurezza;
- il modello organizzativo e gestionale definito per garantire la sicurezza delle informazioni;
- lo Statement formale e le contromisure logiche, fisiche o organizzative necessarie per la concreta realizzazione degli obiettivi di sicurezza prefissati;
- il sistema documentale inerente alla sicurezza delle informazioni.

1. INTRODUZIONE

ART 1) SCOPO DEL DOCUMENTO

1. Il presente documento descrive la Politica per la Sicurezza delle Informazioni della ACSS, intesa come l'insieme delle regole volte ad indirizzare una corretta gestione della sicurezza del Patrimonio Informativo, al fine di contenere i rischi di compromissione della riservatezza, dell'integrità e della disponibilità degli asset informativi, sia in un'ottica di tutela della missione istituzionale che di contrasto agli eventi accidentali o di natura criminosa.

ART 2) CAMPO DI APPLICAZIONE

1. La presente Politica è valida per l'intera ACSS e si applica a tutte le informazioni trattate in qualsiasi modo e qualsiasi formato, a tutti i sistemi di gestione e supporti di memorizzazione utilizzati per il loro trattamento e conservazione.
2. Le informazioni oggetto di protezione si riferiscono, a titolo esemplificativo e non esaustivo, ai seguenti ambiti:
 - a. informazioni associate ai servizi istituzionali erogati e in via di sviluppo;
 - b. know-how strategico;
 - c. informazioni contabili e finanziarie;
 - d. informazioni condivise con gli stakeholder, le Agenzie e le Amministrazioni governative;
 - e. dati personali del personale della ACSS, clienti e soggetti terzi, con riferimento al GDPR, alla normativa nazionale attuativa ed ai Provvedimenti del Garante per la protezione dei dati personali;
 - f. informazioni relative al pubblico che interagisce con la ACSS;
 - g. informazioni inerenti ai processi di procurement e di gestione dei progetti/contratti;
 - h. informazioni legate alla gestione dei servizi e dei sistemi dedicati alla sicurezza ICT;
3. Le risorse cartacee ed informatiche utilizzate per l'elaborazione e la custodia delle informazioni, alle quali si indirizzano gli interventi di tutela, possono comprendere:
 - a. documentazione tecnica o altri documenti contenenti le informazioni della ACSS;
 - b. procedure operative o di supporto;
 - c. piattaforme hardware e software;
 - d. infrastrutture di rete e di telecomunicazione;
 - e. banche dati;
 - f. applicazioni gestionali e di supporto per lo svolgimento dell'attività di ACSS;
 - g. supporti di memorizzazione utilizzati per la conservazione dei dati.

4. Le Informazioni, le risorse informatiche, i supporti digitali e cartacei di archiviazione, costituiscono le cosiddette “Risorse Informative della ACSS”. Le Risorse Informative devono essere protette durante l’intero ciclo di vita fino al momento della loro dismissione.
5. Le regole di seguito descritte sono in vigore a partire dalla data di emissione del presente documento.
6. Sono ammesse deroghe alle regole riportate nel presente documento, solo nei casi in cui ne sia valutato ed accettato il rischio derivante da parte della Direzione della ACSS, con autorizzazione da parte della Direzione stessa.

ART 3) DEFINIZIONI E ACRONIMI

1. Ai fini dell’applicazione della presente Politica devono intendersi le seguenti definizioni:
 - a. **Agenzia per la cybersicurezza nazionale:** l’Agenzia istituita a tutela degli interessi nazionali nel campo della cybersicurezza, di cui all’articolo 5 del decreto-legge 14 giugno 2021, n. 82.
 - b. **Cybersecurity:** l’insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l’integrità e garantendone la resilienza.
 - c. **Collaboratore esterno:** persona fisica che collabora con la ACSS in forza di un contratto libero professionale.
 - d. **CSIRT Italia:** il Computer Security Incident Response Team, di cui all’articolo 8 del decreto legislativo NIS.
 - e. **Decreto-legge:** il decreto-legge 14 giugno 2021, n. 82.
 - f. **Decreto legislativo NIS:** il decreto legislativo 18 maggio 2018, n. 65.
 - g. **Dato Personale:** dato personale ai sensi del GDPR: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
 - h. **Direttiva NIS :** Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell’Unione, recepita in Italia con il decreto legislativo 18 maggio 2018, n.65.
 - i. **Operatore di Servizi Essenziali:** soggetto pubblico o privato, della tipologia di cui all’allegato II al decreto legislativo 18 maggio 2018, n. 65, che soddisfa i criteri di cui all’articolo 4, comma 2, de medesimo decreto.
 - j. **Personale:** dipendente o assimilabile (es. contratti atipici).
 - k. **Strategia nazionale di sicurezza cibernetica:** la strategia di cui all’articolo 6 del decreto legislativo NIS.

- l. **Soggetti terzi:** Fornitori, consulenti, collaboratori esterni, partner che operano con la ACSS in forza di un contratto.
2. Ai fini dell'applicazione della presente Politica devono intendersi i seguenti acronimi:
 - a. **ACN:** Agenzia per la cybersicurezza nazionale.
 - b. **ACSS:** Agenzia di Controllo del Sistema Sociosanitario lombardo.
 - c. **AgID:** Agenzia per l'Italia Digitale.
 - d. **BCP:** Business Continuity Plan.
 - e. **CCNL:** Contratto Collettivo Nazionale di Lavoro.
 - f. **CSIRT:** Computer Security Incident Response Team.
 - g. **LEA:** Livelli Essenziali di Assistenza.
 - h. **NIS:** Network and Information Security.
 - i. **OSE:** Operatore di Servizi Essenziali.
 - j. **PNRR:** Piano Nazionale di Ripresa e Resilienza.
 - k. **RAEE:** Rifiuti e Apparecchiature Elettriche ed Elettroniche.

2. OBIETTIVI DI SICUREZZA

ART 4) OBIETTIVI PER LA SICUREZZA DELLE INFORMAZIONI

1. Considerando la missione istituzionale ed il quadro normativo di riferimento, la ACSS si pone come obiettivo la salvaguardia di:
 - a. la riservatezza delle informazioni, da attuarsi mediante interventi idonei a contrastare il verificarsi di accessi non autorizzati alle informazioni o la diffusione non controllata delle stesse;
 - b. l'integrità delle informazioni, da attuarsi mediante interventi idonei a contrastare il verificarsi di modifiche non autorizzate o il danneggiamento del formato fisico e/o del contenuto semantico delle informazioni;
 - c. la disponibilità delle informazioni, da attuarsi mediante interventi idonei a garantire, ai soggetti autorizzati, l'accesso alle risorse informatiche in tempi utili al compimento della propria missione.
2. Nello specifico la ACSS deve, in via prioritaria:
 - a. definire e applicare un processo di governance della sicurezza delle informazioni, che sia in grado di indirizzare le strategie di trattamento dei rischi in funzione dei cambiamenti derivanti dall'insorgere di nuovi scenari di minaccia, nuove tipologie di vulnerabilità, nuovi fattori di rischio derivanti anche dai cambiamenti organizzativi;
 - b. definire e applicare un processo per l'analisi, la valutazione ed il trattamento dei rischi legati alla cybersecurity;

-
- c. prevedere, a tendere, l'integrazione tra il quadro di riferimento organizzativo e metodologico per l'analisi dei rischi legati alla cybersecurity e gli altri sistemi di gestione dei rischi della ACSS, in modo da garantire una gestione e una valutazione unitaria dei rischi connessi ai servizi istituzionali della ACSS;
- d. definire ed applicare un processo di gestione degli allarmi e degli incidenti di sicurezza informatica, che sia allineato e coerente con la procedura definita ed adottata dall'ACSS per la gestione dei *data breach*;
- e. garantire al personale e ai soggetti terzi un'adeguata conoscenza e un grado di consapevolezza:
- delle problematiche connesse alla sicurezza in termini di minacce, impatti e rischi derivanti da compromissioni della riservatezza, integrità e disponibilità del patrimonio informativo della ACSS;
 - delle regole tecniche ed organizzative per l'utilizzo in sicurezza dei sistemi informativi della ACSS;
 - delle procedure di rilevamento e segnalazione di eventi anomali o sospette violazioni della sicurezza informatica;
 - della normativa applicabile in materia di protezione dei dati personali e delle relative implicazioni, nonché delle modalità di applicazione delle misure previste dalla normativa nonché dalle procedure/istruzioni contenute all'interno del Modello Organizzativo Privacy dell'ACSS;
- f. garantire la conformità ai requisiti cogenti derivanti da normative di legge, dagli standard internazionali e dalle principali best practice di settore;
- g. garantire il rispetto della politica per la sicurezza delle informazioni adottata dalla ACSS.

3. ORGANIZZAZIONE E RESPONSABILITÀ

ART 5) ORGANIZZAZIONE E RESPONSABILITÀ PER LA SICUREZZA DELLE INFORMAZIONI

1. L'organizzazione è funzionale all'individuazione delle politiche dirette alla gestione e al controllo delle misure di sicurezza adottate e si concretizza nella definizione di ruoli, funzioni e responsabilità che concorrono alla realizzazione ed alla gestione del sistema di sicurezza delle informazioni.
2. La ACSS si impegna a definire specifici ruoli e responsabilità per la sicurezza delle informazioni, ad attribuirli alle diverse strutture organizzative interne e a comunicarli affinché siano pienamente compresi ed attuati.
3. I compiti e le aree di responsabilità in conflitto tra loro devono essere separati per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset della ACSS.
4. Nella definizione delle responsabilità associate ai ruoli devono essere previste le attività di gestione dei contatti con le autorità nazionali ed internazionali e con gruppi specialistici e associazioni professionali pertinenti alla sicurezza delle informazioni, nonché le attività di gestione della sicurezza delle informazioni nell'ambito dei progetti.

4. VALUTAZIONE DEI RISCHI

ART 6) SCENARI DI MINACCIA

1. Il progressivo e crescente ricorso alle tecnologie digitali delinea nuovi scenari di minaccia alla cybersecurity che potrebbero compromettere il corretto svolgimento dei servizi, l'integrità degli asset infrastrutturali e determinare violazioni dei diritti e delle libertà delle persone fisiche.
2. D'altra parte, le filiere di approvvigionamento (supply chain) possono a loro volta introdurre nuove minacce e talvolta aumentare il livello di complessità delle azioni di contrasto alle minacce, nonché rallentarne i tempi di attuazione.
3. La ACSS ritiene pertanto fondamentale realizzare un processo di valutazione dei rischi legati alla cybersecurity (di seguito anche rischi cyber) ed alla supply chain, individuando allo stesso tempo le opportune procedure di gestione e riduzione di tali rischi.

5. RISCHI LEGATI ALLA CYBERSECURITY

ART 7) PRINCIPI GENERALI

1. Il processo di valutazione dei rischi cyber e la corrispondente metodologia, affinché siano allineati ai principali standard di riferimento e consentano di ottenere risultati utili, affidabili e rappresentativi della realtà del contesto analizzato, devono soddisfare i seguenti principi generali:
 - a. **Ripetibilità e riproducibilità** - Uno dei risultati del processo di valutazione del rischio cyber è la misurazione del rischio. Tale operazione richiede di essere ripetibile, vale a dire, a parità di ogni altra condizione, si devono ottenere i medesimi risultati, anche in tempi successivi. Da qui la necessità di documentare il metodo utilizzato e almeno le principali assunzioni e semplificazioni.
 - b. **Comprensibilità** - I criteri adottati nell'espressione dei parametri che compongono il rischio (probabilità di accadimento, valore delle informazioni, etc.) e i risultati prodotti devono essere logici e trasparenti, al fine di consentire il riutilizzo dei risultati nella ripetizione del processo di valutazione del rischio cyber.
 - c. **Condivisione** - Il processo di valutazione del rischio cyber deve essere stabilito, gestito e concordato tra i responsabili della ACSS (c.d. stakeholder) ed i valori attribuiti alle informazioni devono essere condivisi tra le diverse Strutture della ACSS interessate.
 - d. **Coerenza** - I valori attribuiti alle informazioni devono essere coerenti con quanto stabilito dalle politiche di sicurezza di alto livello della ACSS.
 - e. **Riutilizzabilità** - I risultati del processo di valutazione del rischio cyber, intermedi o finali, devono poter essere riutilizzabili nel caso in cui l'attività vada ripetuta a seguito di variazioni delle condizioni (valori delle informazioni, minacce, vulnerabilità, etc.) che ne hanno determinato l'esecuzione, anche al fine di realizzare economie di scala. Inoltre, è importante evidenziare che la revisione dell'analisi dei rischi contribuisce all'attuazione del concetto di miglioramento continuo e della sua misurazione. Se necessario, i parametri che definiscono le minacce, così come le vulnerabilità, possono essere ampliati in funzione delle variazioni del contesto di analisi, delle risorse impiegate e delle terze parti che entrano in contatto, per finalità diverse, con l'ambito dell'analisi.
 - f. **Fattibilità in termini temporali** - Le attività correlate al processo di valutazione del rischio cyber devono fornire i risultati in tempi utili, legati ad esempio, al livello di criticità del servizio oggetto di analisi ed al suo ciclo di vita, oppure commisurati con il livello di rischio e/o con il budget allocato secondo anche le regole di sistema.
 - g. **Adeguatezza al livello di consapevolezza dell'Organizzazione** - La complessità di una metodologia per la valutazione del rischio cyber deve essere adeguata al livello di consapevolezza esistente nella ACSS sui temi relativi alla sicurezza delle informazioni, per evitare gli insuccessi derivanti dall'introduzione di sistemi di gestione e processi

non recepiti e lasciati allo stato di evento occasionale, avulso dalla cultura interna alla ACSS.

ART 8) PROCESSO

1. Il processo di valutazione del rischio cyber, in linea con quanto previsto dai principali standard ISO applicabili in materia e con il Framework Nazionale per la Cybersecurity e la Data Protection, deve essere costituito da un insieme di attività ben definite, da compiersi in sequenza ordinata, nell'ambito delle seguenti macro-fasi:

- a. **Context Establishment:** identificazione dell'ambito, dei confini e dell'organizzazione a supporto del processo di valutazione del rischio cyber;
- b. **Risk Assessment:** analisi e valutazione del rischio, che a sua volta deve prevedere le seguenti attività:
 - identificazione e documentazione delle vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione;
 - identificazione e valutazione delle minacce, sia interne che esterne e le relative probabilità di accadimento;
 - identificazione e valutazione dei potenziali impatti sulla mission istituzionale della ACSS;
 - valutazione del rischio in base a quanto emerso dai suddetti punti.

Ai fini della identificazione e valutazione delle minacce e delle vulnerabilità la ACSS deve organizzarsi in modo da ricevere informazioni su minacce, vulnerabilità ed altri dati configurabili come Cyber Threat Intelligence da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing).

- c. **Risk Treatment:** definizione delle strategie per la gestione del rischio e definizione delle modalità operative per l'implementazione delle misure di sicurezza adeguate alla copertura dei rischi rilevati, che a sua volta deve prevedere le seguenti attività:
 - identificazione e comunicazione del livello di rischio tollerato;
 - definizione strategia di trattamento del rischio, con identificazione e prioritizzazione delle misure tecniche ed organizzative necessarie per contenere il rischio valutato entro la soglia di accettazione definita dalla ACSS o soddisfare requisiti di compliance normativa non ancora pienamente soddisfatti.

2. Una caratteristica fondamentale dell'attività di valutazione del rischio cyber è che deve configurarsi come un processo continuo, da cui desumere le azioni da implementare per una gestione del rischio consapevole, adeguata ai valori da proteggere ed in linea, sul piano temporale, con i mutamenti ambientali e tecnologici.

ART 9) RISCHIO TOLLERATO

1. Con riferimento al rischio cyber tollerato, la ACSS, tenendo conto del ruolo dell'Organizzazione quale Operatore Essenziale ai sensi della Direttiva NIS e dei rischi specifici presenti nel settore di appartenenza, ha individuato in un livello basso su una scala di valori a tre livelli (Basso, Medio, Alto), la soglia di rischio accettabile, rispetto alla riservatezza, alla integrità e alla disponibilità delle informazioni.
2. Il livello di rischio tollerato implica che sugli asset esposti a livelli di rischio inferiori o uguali a tale soglia, non sia richiesta l'implementazione di misure di sicurezza specifiche ulteriori rispetto a quanto previsto dalle politiche adottate dall'Ente, dai requisiti normativi e contrattuali e dalle best practice internazionali.
3. Il rispetto delle politiche e dei requisiti normativi, infatti, risulta indipendente dalle attività di analisi del rischio e definisce quindi un insieme minimo di misure di sicurezza.
4. Nell'ambito delle specifiche analisi del rischio su servizi o applicazioni possono essere stabilite soglie di rischio accettate diverse da quelle esplicitate nel presente documento, solo in caso di deroga autorizzata dalla ACSS per comprovate esigenze.

6. RISCHI LEGATI ALLA SUPPLY CHAIN

ART 10) PROCESSI DI GESTIONE DEL RISCHIO INERENTI ALLA CATENA DI APPROVVIGIONAMENTO CYBER

1. La ACSS deve inoltre definire ed implementare i processi di gestione del rischio inerenti alla catena di approvvigionamento cyber.
2. A tal fine i soggetti terzi che forniscono sistemi informatici, componenti e servizi ICT devono essere identificati, prioritizzati e valutati regolarmente da parte della ACSS tramite attività di audit, verifica, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali.
3. Inoltre, i suddetti soggetti terzi devono essere opportunamente coinvolti nelle attività di pianificazione e verifica della risposta e del ripristino agli incidenti aventi impatto sulla sicurezza e sulla continuità operativa dei servizi erogati dalla ACSS.

7. CONTROLLI DI SICUREZZA

ART 11) CONTROLLI DI SICUREZZA DELLE INFORMAZIONI

1. La ACSS ritiene che la sicurezza delle informazioni si ottenga implementando un insieme adeguato e coerente di controlli organizzativi e tecnologici.
2. Di seguito sono formalmente declinati i controlli che costituiscono la presente politica, da attuare per il raggiungimento degli obiettivi di sicurezza definiti dalla ACSS, in base al contesto specifico di riferimento.
3. I controlli sono organizzati in funzione dell'ambito della sicurezza delle informazioni che indirizzano.

8. SICUREZZA DELLE RISORSE INFORMATIVE

ART 12) RISORSE INFORMATIVE

1. Tutte le Risorse Informative della ACSS costituiscono un valore strategico per l'organizzazione e come tali devono essere adeguatamente protette.
2. Nell'ambito delle Risorse Informative, l'informazione assume un ruolo d'importanza primaria costituendo una risorsa critica immateriale, necessaria ai processi di pianificazione, organizzazione, esecuzione e controllo delle attività condotte dalla ACSS.

ART 13) INVENTARIO DEGLI ASSET

1. L'inventario delle risorse informative è necessario per monitorare l'obsolescenza delle risorse utilizzate, pianificare il loro ammodernamento, rinnovare le licenze e programmare gli investimenti in tecnologie dell'informazione.
2. L'inventario deve comprendere:
 - a. **Informazioni:** database e archivi cartacei, documentazione di sistema, manuali per l'utente, materiale per l'addestramento, procedure operative o di supporto, ecc.;
 - b. **Risorse software:** software di base ed applicativo, strumenti di sviluppo, programmi di utilità, ecc.;
 - c. **Risorse hardware:** apparecchiature informatiche (ad es. server fisici e virtuali, client fissi e portatili, monitor, sistemi di backup e restore, ecc.), apparecchiature di comunicazione (ad es. router, segreterie telefoniche, ecc.), supporti magnetici (ad es.

- nastri e dischi), altre apparecchiature tecniche (ad es. alimentazioni elettriche, unità di climatizzazione, ecc.);
- d. **Sistemi informativi esterni** all'organizzazione utilizzati nell'ambito della ACSS (ad es. cloud);
 - e. **Flussi di dati e comunicazioni** inerenti all'organizzazione;
 - f. **Locali:** i luoghi fisici ove sono custodite le informazioni, le risorse software e hardware e dove vengono effettuate le elaborazioni;
 - g. **Capitale umano:** personale e soggetti terzi che operano presso la ACSS.
3. Le risorse hardware inerenti alla postazione di lavoro (personal computer, periferiche connesse, videoterminale) sono noleggiate da ACSS nell'ambito della "Convenzione per l'affidamento del servizio di gestione delle postazioni di lavoro e servizi connessi e opzionali per Regione Lombardia e gli enti del sistema regionale di cui all'art. 1 della Legge Regionale n. 30/2006 e s.m.i. che utilizzano l'infrastruttura di rete di Regione Lombardia e Arexpo, Giunta Regionale e Consiglio Regionale" e gestite da Aria - Engineering. Il Sistema Operativo e alcuni software sono inclusi all'interno della specifica fornitura, quali ad esempio DigitalSign, Cisco AnyConnect, Avamar Client, Ego Secure Agent by Matrix 42, Data Protection.
- La connettività di rete e la telefonia fissa sono fornite presso la sede di Palazzo Sistema da un fornitore esterno, l'utilizzo è regolamentato secondo quanto riportato nei paragrafi 5.5. e 5.6 del Decreto di Regione Lombardia n. 13455 del 22 settembre 2022 (allegato al presente documento).
4. Infine, devono essere identificati e catalogati tutti i trattamenti di dati personali effettuati dalla ACSS ai sensi del GDPR. (Registri dei trattamenti di dati personali).
 5. Tutte le Risorse Informative sono di proprietà della ACSS, a cui è riservato ogni diritto ai sensi della normativa vigente sulla Protezione del diritto d'autore, laddove applicabile.
 6. La riproduzione, la pubblicazione e la distribuzione, totale o parziale, delle Risorse Informative sono espressamente vietate in assenza di una autorizzazione scritta da parte del proprietario.
 7. ACSS ha implementato in tutte le sue componenti la Piattaforma Microsoft 365, per il pieno adempimento alla normativa privacy, tutti i dati sono quindi stati pertanto migrati su tale Cloud, l'accesso tramite connessioni esterne può avvenire solo tramite sistemi MFA.

ART 14) UTILIZZO DEGLI ASSET

1. Il personale utilizza le Risorse Informative di proprietà della ACSS nei limiti dell'autorizzazione assegnata e per esclusive finalità lavorative.
2. Tale utilizzo deve sempre ispirarsi ai principi di diligenza, correttezza e riservatezza che sono alla base di ogni atto o comportamento posto in essere nell'ambito del rapporto professionale, in coerenza con le vigenti normative, e tenendo sempre presente l'interesse collettivo al risparmio delle risorse pubbliche.

3. La ACSS, ammette l'uso degli strumenti informatici, ed in particolare di Internet, per motivi personali soltanto in caso di urgenza e comunque non in modo ripetuto e per periodi di tempo brevi, e in ogni caso sempre nel rispetto del principio di riservatezza e delle esigenze di funzionalità della rete e di semplificazione dei processi lavorativi.
4. La ACSS perseguirà a norma di legge e del vigente contratto di lavoro, il personale che utilizza in modo non appropriato i sistemi di elaborazione delle informazioni, poiché l'eventuale esposizione al rischio impedirebbe alla ACSS il corretto svolgimento delle proprie attività istituzionali ed il rispetto delle normative cogenti applicabili.
5. Il personale della ACSS, oltre che al rispetto del Codice di Comportamento (Deliberazione del Comitato di Direzione n°2 del 21/12/2022), è tenuto ad osservare le indicazioni inserite nelle presenti Politiche sulla sicurezza delle informazioni e regolamenti nell'utilizzo delle dotazioni informatiche, quali:
 - a. Lasciare sempre la postazione/scrivania libera da informazioni sensibili (Clean Desk Policy);
 - b. Utilizzare il privacy screen protect quando si lavora in luoghi condivisi o sui mezzi di trasporto;
 - c. Non lasciare incustodito il PC o altri dispositivi di lavoro;
 - d. Evitare di scaricare in autonomia programmi e/o applicazioni;
 - e. Non utilizzare stazioni di ricarica USB pubbliche;
 - f. Non utilizzare reti pubbliche;
 - g. Utilizzare solo dispositivi autorizzati, software e strumenti forniti dall'agenzia per il lavoro;
 - h. Lavorare in un ambiente sicuro e mantenere la sicurezza fisica (es: utilizzo del cavo di sicurezza, utilizzo dello schermo protettivo, bloccare manualmente lo schermo del computer nel caso in cui ci si allontani dalla postazione);
 - i. Utilizzare solo strumenti di file sharing sicuri e forniti dall'Organizzazione (evitare servizi come WeTransfer, Dropbox, Google Drive, ecc.);
 - j. Condividere file/cartelle/documenti solo quando strettamente necessario;
 - k. Non condividere mai l'intero disco, ma solo i singoli elementi, per un periodo di tempo limitato;
 - l. Non salvare, su alcun dispositivo esterno, file con le informazioni dell'Ente;
 - m. Nell'ambito di dispositivi e supporti mobili e rimovibili, si raccomanda di:
 1. Eliminare i dati e renderli completamente illeggibili in modo che nessun altro possa accedere alle informazioni;
 2. Conservare al loro interno solo informazioni inerenti alle attività lavorative;
 - n. In caso di smart working, si raccomanda di:
 1. Utilizzare sempre e solo le postazioni di lavoro fornite dall'Agenzia;
 2. Evitare la navigazione su pagine Internet poco sicure o malevole;
 3. Tutelare le informazioni anche nel contesto familiare;

4. Utilizzare i dispositivi esclusivamente per attività lavorative; Assicurarsi che la rete domestica sia sicura (ad es. password forte/univoca, crittografia WPA2 o WPA3);
 - o. In caso di lavoro in luoghi pubblici, si raccomanda di:
 1. Evitare la navigazione su pagine internet poco sicure o malevole;
 2. Tutelare le informazioni anche nel contesto familiare;
 3. Utilizzare i dispositivi esclusivamente per attività lavorative;
 4. Assicurarsi che la rete domestica sia sicura (ad es. password forte/univoca, crittografia WPA2 o WPA3)
5. A tal fine devono essere predisposte idonee istruzioni per il personale, contenenti indicazioni circa le modalità di corretto utilizzo delle Risorse Informative nonché le responsabilità, anche giuridiche derivanti, in caso di inosservanza. ACSS ha aderito al progetto Syllabus al quale tutti i dipendenti sono stati censiti e invitati nello svolgere tale attività formativa. Presso ACSS sono stati svolti dei corsi di formazione relativi alla politica della sicurezza delle informazioni e fornite istruzioni operative.

ART 15) CLASSIFICAZIONE E TRATTAMENTO DELLE INFORMAZIONI

1. Le informazioni trattate nell'ambito delle attività della ACSS devono essere tutelate e gestite sulla base del loro valore in termini di impatti derivanti dalla perdita della disponibilità, integrità e riservatezza delle stesse.
2. Tutte le informazioni trattate dalla ACSS devono essere classificate attribuendo alle stesse un grado di criticità utile a determinarne il livello di protezione.
3. La protezione deve riguardare tutte le fasi connesse alla gestione dell'informazione: generazione, raccolta, classificazione, emissione, oscuramento ove previsto dalle norme (cfr. ad esempio e s.m.i.), ricezione, custodia, divulgazione, consultazione, riclassificazione, modifica, conservazione e distruzione.
4. A tal fine, devono essere predisposte da ACSS adeguate politiche contenenti, in conformità alle esigenze istituzionali ed alla normativa vigente in materia di tutela del trattamento dei dati personali:
 - a. i criteri per la classificazione delle informazioni;
 - b. le misure minime di sicurezza da adottare per il trattamento delle informazioni classificate e la relativa etichettatura.

ART 16) ASSEGNAZIONE DI PRIORITÀ AGLI ASSET

1. Gli asset della ACSS (cfr. Art. 13) devono essere prioritizzati in base alla classificazione (cfr. Art. 15), criticità e valore per la mission dell'organizzazione, delle informazioni da essi trattate.

2. Inoltre, devono essere identificate e rese note le interdipendenze e le funzioni fondamentali per la fornitura di servizi critici. Nella fattispecie ACSS non eroga servizi critici.

ART 17) UTILIZZO DI SUPPORTI E DISPOSITIVI INFORMATICI DELLA ACSS PER LA MEMORIZZAZIONE

1. La memorizzazione delle informazioni deve essere effettuata utilizzando le applicazioni istituzionali preposte (es. Sharepoint, OneDrive) ed è pertanto necessario limitare la memorizzazione di informazioni su supporti e dispositivi diversi come ad es. dischi locali del PC, memorie esterne, ecc.
2. È comunque necessario regolamentare la memorizzazione di informazioni su supporti e dispositivi informatici della ACSS (dischi locali del PC, memorie esterne, ecc.) prevedendo un processo formale di autorizzazione nel caso di memorizzazione di dati personali ai sensi del GDPR o critici della ACSS.
3. Inoltre, i supporti e i dispositivi informatici della ACSS per la memorizzazione, incluse le memorie esterne (es. cd rom, dvd, hard disk portatili, chiavi USB), devono essere protetti dai rischi di accesso non autorizzato e/o manomissioni, in funzione della classificazione delle informazioni in essi contenuti.

ART 18) UTILIZZO DI SUPPORTI E DISPOSITIVI PERSONALI

1. Non è consentito l'utilizzo di supporti e dispositivi personali ai fini dello svolgimento dell'attività lavorativa, fatto salvo situazioni specifiche che dovranno essere di volta in volta autorizzate dalla ACSS valutandone il rischio derivante.

ART 19) LAVORO DA REMOTO

1. La ACSS è consapevole che il lavoro da remoto può risultare fondamentale per favorire l'efficienza e l'efficacia delle attività in particolari situazioni aziendali e sociosanitarie.
2. Tuttavia, tale modalità può comportare rischi anche significativi per la sicurezza delle informazioni della ACSS e pertanto deve essere opportunamente regolamentato, nel rispetto di quanto consentito dalla legge vigente e dai contratti di lavoro.

9. SICUREZZA NELL'AMBITO DELLE RISORSE UMANE

ART 20) INDIVIDUAZIONE DEL PERSONALE

1. Tutto il personale della ACSS ed i collaboratori esterni, con particolare riferimento a quelli destinati a ricoprire ruoli di gestione della sicurezza, devono essere attentamente individuati, in funzione delle esigenze istituzionali della ACSS e sulla base di criteri di affidabilità e competenza professionale.
2. Una volta individuato il personale si procederà ad assegnare i compiti al personale dedicato alla sicurezza delle informazioni, oltre alla struttura organizzativa di appartenenza, specifici ruoli operativi e profili professionali, previo adeguato percorso formativo ad hoc.

ART 21) RESPONSABILITÀ DEL PERSONALE E DEI COLLABORATORI ESTERNI

1. Tutto il personale e i collaboratori esterni devono essere informati delle proprie responsabilità, anche giuridiche, derivanti da violazioni, frodi o dall'utilizzo improprio delle Risorse Informative della ACSS, nonché da uno scorretto trattamento delle informazioni e dei dati personali.
2. I rapporti interpersonali ed i comportamenti, a tutti i livelli organizzativi, devono essere improntati a principi di onestà, correttezza, trasparenza, riservatezza, imparzialità, diligenza, lealtà e reciproco rispetto (per il personale si rimanda al Contratto Collettivo Nazionale di Lavoro, al Regolamento recante codice di comportamento dei dipendenti pubblici, ai codici deontologici dei rispettivi ordini professionali ed al Regolamento per i procedimenti disciplinari relativi al personale dipendente del comparto della dirigenza della ACSS, mentre per i collaboratori esterni ai contratti individuali).

ART 22) SENSIBILIZZAZIONE E FORMAZIONE

1. Tutto il personale ed i collaboratori esterni devono essere adeguatamente informati e sensibilizzati in merito alle politiche e alle procedure operative di sicurezza pertinenti alla propria attività lavorativa.
2. In particolare, devono essere definiti, erogati e aggiornati piani formativi mirati ad accrescere il grado di consapevolezza e di sensibilizzazione sugli obiettivi di sicurezza prefissati e sulle principali problematiche di sicurezza delle informazioni.
3. I piani di formazione devono prevedere un approfondimento specifico su:
 - a. politiche, procedure e linee guida di sicurezza adottate dalla ACSS;

- b. ruoli organizzativi previsti per la gestione delle tematiche di sicurezza delle informazioni, responsabilità del personale coinvolto e principali implicazioni di eventuali non conformità sulla sicurezza delle risorse della ACSS;
- c. principali tematiche e controlli di sicurezza delle informazioni, inclusa la cybersecurity.

ART 23) CESSAZIONE E VARIAZIONE DEL RAPPORTO DI LAVORO

1. Le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o variazione del rapporto di lavoro devono essere definiti, comunicati al personale ed ai collaboratori esterni e resi effettivi.

10.SICUREZZA NELLE RELAZIONI CON I SOGGETTI TERZI

ART 24) CONTROLLI GENERALI

1. Tutti i soggetti terzi devono essere informati delle proprie responsabilità, anche giuridiche, derivanti da violazioni della sicurezza o dall'utilizzo improprio delle Risorse Informative della ACSS, qualora l'attività individuata possa comportare l'accesso a tali risorse.
2. È necessario garantire la sicurezza delle Risorse Informative accedute ed utilizzate anche dai soggetti terzi che a qualsiasi titolo, svolgono, anche temporaneamente, attività di lavoro per la ACSS.
3. La ACSS, come evidenziato nelle Linee Guida per la sicurezza nel procurement ICT, è consapevole che i soggetti terzi, in relazione alla natura dei servizi offerti, possono accedere al patrimonio informativo della ACSS, introducendo potenziali rischi cyber in grado di vanificare, o comunque rendere meno efficaci, le misure prese dalla ACSS per tutelare il proprio patrimonio informativo. Risulta pertanto fondamentale definire ed attuare procedure per garantire la sicurezza delle informazioni in relazione all'approvvigionamento di beni e servizi informatici (procurement ICT) che indirizzino tutte le fasi di approvvigionamento (prima, durante e dopo).
4. È necessario garantire la sicurezza delle Risorse Informative rese disponibili all'utilizzo da parte di soggetti terzi ai fini dell'esecuzione degli specifici obblighi contrattuali e nei limiti dell'autorizzazione assegnata.
5. A tal fine, devono essere predisposte:
 - a. adeguate politiche e procedure contenenti i criteri e le modalità per la gestione delle Risorse Informative da parte dei soggetti terzi, in conformità alle esigenze istituzionali ed alle normative vigenti. Tali politiche e procedure devono risultare adeguate

- rispetto ai rischi, accidentali e/o intenzionali, di distruzione, perdita, divulgazione, alterazione e accesso non autorizzato delle Risorse Informative della ACSS;
- b. idonee istruzioni contenenti indicazioni circa le modalità di corretto utilizzo delle Risorse Informative nonché le responsabilità, anche giuridiche, derivanti in caso di inosservanza.

ART 25) CLAUSOLE CONTRATTUALI

1. Devono essere previste specifiche clausole per garantire la riservatezza e la non-divulgazione delle informazioni della ACSS accedute ed utilizzate dai soggetti terzi, secondo quanto previsto dalle normative vigenti.
2. Gli accordi con i soggetti terzi devono necessariamente contemplare tutti i requisiti necessari ad assicurare la protezione delle Risorse Informative della ACSS e devono indirizzare l'intera catena di approvvigionamento a garanzia del mantenimento della sicurezza delle informazioni in tutte le fasi.
3. Inoltre, i soggetti terzi devono essere informati sulle politiche, le procedure e le istruzioni di sicurezza della ACSS relativamente al tipo di attività previste dal contratto.

ART 26) MONITORAGGIO, REVISIONE E GESTIONE DEL CAMBIAMENTO DEI SERVIZI DELLE TERZE PARTI

1. I servizi delle terze parti devono essere regolarmente monitorati, riesaminati e verificati al fine di rilevare scostamenti rispetto agli accordi contrattuali nonché gestire eventuali cambiamenti alla fornitura di tali servizi (in occasione ad esempio di interventi migliorativi, cambiamenti tecnologici o delle politiche e delle procedure di sicurezza, rivalutazione dei rischi).

ART 27) SICUREZZA DELLE INFORMAZIONI PER L'UTILIZZO DEI SERVIZI CLOUD

1. Devono altresì essere definite politiche specifiche e relativi processi atti ad indirizzare e gestire la sicurezza delle informazioni lungo tutto il ciclo di vita dei servizi cloud.

11.SICUREZZA FISICA E AMBIENTALE

ART 28) PROTEZIONE DA MINACCE DI TIPO FISICO ED AMBIENTALE

1. Tutte le Risorse Informative, cartacee ed informatiche, della ACSS devono essere protette dai rischi di accesso non autorizzato, sottrazione, manomissioni e danneggiamento derivanti da minacce di tipo fisico ed ambientale.
2. I sistemi di sicurezza fisica per la protezione delle aree, degli uffici, delle stanze e degli impianti dai danni derivanti da incendi, allagamenti, esplosioni ed altre forme di disastro naturale o umano, in coerenza con le risorse tecnico-strutturali, economiche e logistiche aziendali sono previsti nell'ambito della Convenzione sugli spazi con la Giunta Regionale (Determinazione del Direttore dell'Agenzia n.119 del 21/12/2018 - *"Approvazione nuovo schema di Accordo per la concessione spazi nelle sedi istituzionali agli enti facenti parte del Sistema regionale ai sensi della LR 30/2006 e partecipate"*), che garantisce gli spazi, le attività di manutenzione ordinaria e straordinaria, la gestione dei sistemi di sicurezza e vigilanza esterna e interna, la gestione delle utenze e i servizi infotelematici e di comunicazione.
3. I sistemi di sicurezza adottati devono essere regolarmente verificati e mantenuti.
4. Devono essere predisposte idonee procedure organizzative per la regolamentazione ed il controllo dell'accesso ai sistemi informatici da parte del personale e dei soggetti terzi autorizzati alla gestione/manutenzione degli stessi.

ART 29) SICUREZZA DELLE AREE

1. Il perimetro di sicurezza delle aree contenenti le informazioni critiche e le strutture di elaborazione delle informazioni deve essere chiaramente definito e controllato.
2. Quando non presidiate, le aree devono essere tenute chiuse e controllate periodicamente.

ART 30) CONTROLLO DEGLI ACCESSI FISICI

1. Tutte le risorse informative devono essere ubicate prevalentemente in edifici con accesso a personale preventivamente autorizzato. L'accesso fisico è controllato e consentito solo al personale e agli eventuali soggetti terzi e visitatori preventivamente identificati ed autorizzati, solo per i compiti specifici e limitati alle attività di competenza.
2. Il personale che fornisce servizi di supporto e di manutenzione è autorizzato all'accesso nelle aree laddove necessario e in maniera limitata (anche temporalmente).

3. I diritti di accesso devono essere regolarmente verificati e revocati al personale ed ai soggetti terzi che lasciano gli incarichi per i quali era previsto l'ingresso alle aree stesse.
4. A tal fine devono essere predisposte idonee procedure per la regolamentazione ed il controllo degli accessi alle aree e ai locali della ACSS.

ART 31) SICUREZZA DEGLI UFFICI, DELLE STANZE E DEGLI STRUMENTI DI LAVORO

1. Gli uffici e le stanze devono essere protetti in funzione della classificazione delle risorse informative ivi trattate e custodite (cfr. Art. 15), pertanto si raccomanda il personale a tenere chiusi a chiave gli uffici.
2. L'accesso agli uffici ed alle stanze deve essere consentito solo al personale autorizzato, ai soggetti terzi ed ai visitatori preventivamente identificati.
3. Gli strumenti di lavoro devono essere fisicamente protetti dai rischi di accesso non autorizzato e da conseguenti manomissioni o furti. A tal fine, quando non posti sotto il diretto controllo dell'assegnatario, personal computers e periferiche video devono rimanere assicurati alla postazione di lavoro con il sistema di sicurezza Kensington.
4. Il controllo degli accessi agli strumenti da parte del personale e dei soggetti terzi autorizzati alla gestione/manutenzione degli stessi viene gestito dalle articolazioni organizzative di ACSS sulla base della competenza dell'intervento
5. L'accesso agli uffici e alle dotazioni informatiche di ACSS è protetto dal sistema di vigilanza interna ed esterna di Palazzo Sistema e dall'assenza dell'accesso aperto al pubblico, in quanto ogni accesso di esterni viene registrato e controllato nel servizio di portineria della sede di ACSS.

ART 32) LAVORARE IN AREE SENSIBILI

Non presenti aree sensibili

ART 33) SICUREZZA DELLE AREE DI CARICO E SCARICO

Non presenti aree destinate a tale scopo negli uffici di ACSS.

ART 34) EQUIPAGGIAMENTO DI SICUREZZA

Il Personale di ACSS non necessita di equipaggiamento di sicurezza in quanto non ha accesso a locali tecnici.

ART 35) SICUREZZA DEL CABLAGGIO

1. La sicurezza e la corretta posa del cablaggio dedicato alle postazioni di lavoro deve essere garantita dal personale tecnico di cui alla convenzione relativa alle postazioni di lavoro.

12.SICUREZZA DELLE ATTIVITÀ OPERATIVE

ART 36) PROCEDURE OPERATIVE E RESPONSABILITÀ

1. Le procedure operative inerenti ai processi di gestione dei sistemi informatici devono essere documentate, mantenute e rese facilmente disponibili a tutto il personale incaricato di attuarle.
2. Qualsiasi modifica inerente ai sistemi e agli strumenti di gestione delle informazioni deve essere autorizzata, controllata e documentata.
3. Le responsabilità del controllo devono essere affidate a strutture o a personale esterno alle aree operative, onde ridurre le opportunità di modifiche non autorizzate o accidentali e manomissioni delle risorse informative della ACSS.
4. Gli ambienti di sviluppo, di produzione e test devono essere separati al fine di ridurre al minimo i rischi di accessi o modifiche non autorizzate o anche accidentali dei relativi sistemi informativi.
5. ACSS individua all'interno dell'organizzazione soggetti deputati al controllo delle aree operative con particolare riferimento al ruolo di amministratore di sistema.

ART 37) PROTEZIONE DA MALICIOUS SOFTWARE

1. L'integrità delle informazioni e delle risorse informatiche deve essere preservata dalla possibile compromissione da parte di software malevolo (ad esempio virus, worm, trojan horses).
2. Al riguardo è necessario definire:

- a. una politica di formazione ed informazione del personale e degli eventuali soggetti terzi sui danni potenziali arrecati alle Risorse Informative, legati all'introduzione di software malevolo;
 - b. idonee contromisure per l'individuazione di software malevolo nei sistemi informatici, nonché per il ripristino delle risorse eventualmente danneggiate. In tal senso, le postazioni di lavoro devono disporre almeno di un sistema antivirus aggiornato allo stato dell'arte.
3. I programmi antivirus devono essere gestiti e controllati in maniera tale da assicurarne una capillare diffusione ed un frequente aggiornamento.
4. Devono essere definite idonee contromisure atte a gestire gli eventi dannosi (isolamento, ripristino) ed a fornire supporto agli utenti coinvolti.

ART 38) SOFTWARE NON AUTORIZZATO

1. Deve essere vietato l'utilizzo di software non espressamente autorizzati. Tutti i software installati sui sistemi informativi devono essere conformi ai termini delle licenze (vincoli d'uso) ed utilizzato per esclusive finalità lavorative.
2. Al riguardo è necessario impedire l'incauto prelievo di software e di file da computer remoti o la loro installazione non autorizzata in computer della ACSS.
3. Tutto il personale deve essere reso consapevole dei danni potenziali arrecati alle Risorse Informative dall'introduzione di software non autorizzati, diversi da quelli standard in dotazione.
4. Devono essere definite idonee politiche e procedure di sicurezza e previsti strumenti per la prevenzione e l'individuazione di software non autorizzato nel sistema informatico nonché per il ripristino delle risorse eventualmente danneggiate.

ART 39) BACK-UP

1. Per i sistemi presenti sui Data Center devono essere previste, anche in conformità alle normative vigenti, adeguate politiche e procedure di back-up per preservare l'integrità e garantire la disponibilità delle informazioni (ad esempio in caso di manomissioni, atti vandalici, contaminazione da virus, perdita o distruzione anche involontaria).
2. Le procedure devono riguardare la verifica della corretta esecuzione dei back-up, il mantenimento di un elenco delle copie effettuate, l'archiviazione sicura, i criteri ed i tempi per la conservazione dei supporti di memorizzazione (dischi, nastri ecc.), i meccanismi e le modalità per la cancellazione sicura delle informazioni in caso di distruzione, smaltimento o riutilizzo dei supporti.

3. Laddove il back-up venga effettuato localmente nell'ambito dell'ufficio devono essere impartite al personale e agli eventuali soggetti terzi, le idonee istruzioni tecniche ed organizzative. Tali istruzioni devono indicare gli strumenti e le modalità con cui effettuare le copie di sicurezza, l'elenco delle banche dati e degli archivi per i quali è richiesta la copia, la sequenza temporale e la finestra operativa per garantire che i dati copiati siano tra loro congruenti. Tale attività deve comunque considerarsi transitoria in un'ottica di utilizzo di sistemi completamente cloud.

ART 40) SICUREZZA DELLA RETE DATI

1. La rete dati deve essere adeguatamente gestita e controllata. I sistemi e le applicazioni utilizzati nella rete dati devono essere mantenuti in sicurezza, incluse le informazioni in transito.
2. Devono essere definite politiche e procedure per la sicurezza della rete dati. Tutte le attività di manutenzione devono essere tracciate e verificate.
3. Gli aggiornamenti di sicurezza, i livelli di servizio ed i requisiti per la gestione dei servizi di rete devono essere identificati e formalizzati in specifici accordi contrattuali ogniquale volta la gestione dei servizi sia affidata all'esterno.
4. Le prestazioni della rete dati devono essere controllate per verificare la conformità della gestione rispetto ai parametri attesi.
5. Tutte le attività inerenti alla sicurezza della rete dati sono svolte da fornitori esterni e regolamentati secondo quanto indicato nel Decreto di Regione Lombardia n. 13455 del 22 settembre 2022 – Regole per i Servizi Infotelematici della giunta regionale.

ART 41) SICUREZZA NELLO SCAMBIO DI INFORMAZIONI

1. La gestione dello scambio di informazioni deve avvenire tramite la piattaforma Microsoft 365 o tramite il sistema di protocollo di ACSS. Nei casi in cui ciò non è attuabile, al fine di evitarne la perdita, la modifica o l'uso improprio delle informazioni verranno effettuate secondo il contesto organizzativo aziendale.
2. Gli eventuali supporti contenenti le informazioni devono essere protetti da accessi non autorizzati, manomissioni o alterazioni durante il trasporto.

3. Le informazioni critiche per la ACSS contenute nei messaggi elettronici devono essere protette dai rischi di frode, accesso non autorizzato, alterazioni o distruzione mediante l'adozione di idonei sistemi di sicurezza.
4. Le informazioni scambiate nelle transazioni elettroniche devono essere protette al fine di prevenire trasmissioni incomplete, reindirizzamenti, accessi non autorizzati, alterazioni, duplicazioni non autorizzate dei messaggi.
5. Devono essere definite ed attuate specifiche procedure di sicurezza per garantire la protezione delle informazioni correlate ai sistemi a supporto dei servizi istituzionali, in funzione della loro classificazione.
6. Deve essere prevista un'idonea procedura contenente le raccomandazioni sulla sicurezza della rete interna, le regole per la navigazione in Internet e le indicazioni per l'uso appropriato del servizio di posta elettronica. Tale aspetto è regolamentato secondo quanto indicato nel Decreto di Regione Lombardia n. 13455 del 22 settembre 2022 – Regole per i Servizi Infotelematici della giunta regionale.
7. Si raccomanda al personale che accede alle dotazioni informatiche e alla rete Internet di ACSS di non scaricare allegati o cliccare su link presenti in e-mail di phishing, in quanto potenziali veicoli per la diffusione di malware sui sistemi, evitare di navigare su siti web che non forniscono protocollo https e non utilizzare i dispositivi di lavoro per scaricare programmi non autorizzati e non utili ai fini dell'attività lavorativa.
8. Le pagine social potrebbero esser oggetto di attacchi volti a carpire e trafugare informazioni sensibili dell'Organizzazione, con conseguenze rilevanti per il business della stessa. L'utilizzo dei social network non è consentito, fatto salvo per le eventuali pagine istituzionali e i soggetti espressamente autorizzati alla gestione. Nell'utilizzo privato, si raccomanda di non:
 - a. pubblicare foto relative agli ambienti di lavoro e/o riservati, potrebbero fornire informazioni utili ad eventuali attaccanti;
 - b. condividere informazioni sui progetti o sulle attività ai quali si sta partecipando;
 - c. pubblicare, senza autorizzazione alla divulgazione, informazioni sull'Organizzazione o divulgare documenti di lavoro tramite i social network.

ART 42) MONITORAGGIO

1. Le informazioni inerenti alle attività effettuate dagli utenti dei sistemi ICT della ACSS e più in generale agli eventi che possono compromettere la sicurezza delle risorse informative devono essere tracciate (ad esempio tramite file di log), memorizzate e conservate per un periodo di tempo ritenuto idoneo a supportare la risoluzione di problemi inerenti al

funzionamento dei sistemi ICT, le future attività di accertamento e la “gestione degli incidenti”, nel rispetto della normativa vigente (es. GDPR, Statuto dei lavoratori).

2. Analogamente, devono essere definite procedure per il monitoraggio e il successivo accertamento del corretto utilizzo degli strumenti di elaborazione delle informazioni, nel rispetto della normativa vigente (es. Statuto dei lavoratori).
3. Gli strumenti di monitoraggio devono essere protetti contro i rischi di accesso non autorizzato e/o di alterazione.
4. I guasti ed i malfunzionamenti devono essere tracciati ed analizzati e devono essere intraprese opportune azioni correttive, nel rispetto dei livelli di servizio definiti contrattualmente o in assenza di questi, nel minore tempo possibile per non arrecare degni degni prestazioni o rallentamenti delle attività di monitoraggio.

ART 43) CRITTOGRAFIA

1. Ai fini dell'utilizzo della crittografia per la protezione delle informazioni, qualora richiesto, deve essere:
 - a. definita una specifica politica di sicurezza;
 - b. predisposta ed attuata un'adeguata procedura per la gestione delle chiavi crittografiche.
 - c. Lo strumento utilizzato per la crittografia deve essere fornito dall'Agenzia. (es. Digital Sign).
2. Tali politiche e procedure devono risultare conformi alle vigenti normative nazionali ed agli standard internazionali in merito.

ART 44) SMALTIMENTO E CANCELLAZIONE SICURA DEI DATI

1. Le informazioni trattate presso la ACSS devono essere cancellate o distrutte nei casi in cui:
 - a. non siano più utili al raggiungimento delle finalità lavorative (ad es. copie di documentazione obsolete o relative a versioni superate o in soprannumero);
 - b. siano relative alla cessazione per qualsiasi causa di trattamenti di dati personali/critici non più necessari, pertinenti o eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;
 - c. gli scopi per le quali sono state raccolte e trattate non siano più determinati, espliciti e legittimi oppure siano diventate incompatibili con tali scopi;
 - d. risultino scaduti i termini legittimi di conservazione anche con riferimento al tempo necessario agli scopi per i quali sono stati raccolti o successivamente trattati, siano essi determinati da norme di legge generali e/o di settore (ad es. dieci anni per la conservazione delle scritture contabili) oppure dalle finalità per le quali i dati sono stati raccolti o in relazione alle quali devono essere conservati (ad es. contenziosi). La

- ACSS per la conservazione dei dati si attiene ai tempi previsti dal Titolare e Massimario del Sistema Sanitario e Sociosanitario di Regione Lombardia, che deve pertanto essere rispettato;
- e. l'Interessato ne richieda la cancellazione, nell'esercizio dei propri diritti, nei casi applicabili e previsti dalle norme in materia di privacy;
 - f. il supporto elettronico sul quale sono memorizzate sia destinato allo smaltimento o dismissione, oppure quando sia destinato al reimpiego da parte di terzi.
2. A tal fine il gestore delle postazioni di lavoro adotta una procedura operativa per la cancellazione e distruzione sicura delle informazioni in linea con quanto previsto in materia dal Garante per la protezione dei dati personali. Tali procedure devono garantire la non recuperabilità delle informazioni e la tecnica di cancellazione deve tenere conto della tipologia di supporto elettronico utilizzato e della classificazione delle informazioni in esso contenute.
3. Deve inoltre essere definito il processo di distruzione sicura di supporti rientranti nella categoria RAEE (Rifiuti e Apparecchiature Elettriche ed Elettroniche), nell'ambito del quale deve essere garantito il rispetto delle normative ambientali "relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti" e di tutte le altre fonti normative in materia.

13.CONTROLLO DEGLI ACCESSI

ART 45) ACCESSO ALLE INFORMAZIONI E ALLE RISORSE ICT

1. Deve essere protetto e controllato l'accesso alle informazioni ed alle risorse ICT utilizzate per la loro elaborazione.
2. A tal fine occorre definire formalmente e aggiornare periodicamente una politica di controllo degli accessi sulla base delle esigenze istituzionali della ACSS e dei requisiti di sicurezza delle informazioni.
3. Il gestore dell'Active Directory di concerto con il responsabile della Sicurezza delle Informazioni di ACSS adotta tutte le indicazioni normative e le indicazioni fornite da Agid in merito alla gestione corretta dell'Active directory di ACSS.

ART 46) REVISIONE DEI DIRITTI DI ACCESSO

1. Tutti i diritti di accesso assegnati al personale, nonché ai soggetti terzi ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali, devono essere regolarmente controllati ed aggiornati.

2. Deve essere prevista la modifica/revoca dei diritti d'accesso quando vengono meno le condizioni per le quali sono stati assegnati (ad esempio a seguito della cessazione del rapporto lavorativo o di cambio della mansione).

14. ACCESSI LOGICI

ART 47) GESTIONE DELLE CREDENZIALI DI ACCESSO

1. Devono essere definiti politiche, procedure ed istruzioni per la gestione delle credenziali di accesso in conformità alle normative vigenti, con particolare riferimento a quelle in materia di protezione dei dati personali. In tal senso:
 - a. il codice identificativo (user-id) deve essere univoco e non riutilizzabile successivamente;
 - b. le password devono essere individuali e l'utente è responsabile della loro riservatezza.
2. Inoltre, devono essere definiti standard per la maggiore complessità delle password in proporzione al livello di criticità dell'informazione e al livello di criticità dei sistemi sotto il profilo della sicurezza (es. minimo 8 caratteri, almeno un carattere speciale, almeno un carattere maiuscolo, ecc.).
3. Al fine di ridurre la proliferazione delle password e delle credenziali di accesso, l'agenzia adotta l'integrazione con Activity Directory tra i diversi applicativi a disposizione dell'ACSS per la determinazione di un'unica password utilizzabile per tutti gli applicativi, basata sull'autenticazione a più fattori (MFA), o autenticazione forte, che per garantire la sicurezza richiede due o più fattori di verifica dell'identità di un utente oltre alla combinazione di user-ID e password. Gli applicativi integrati al dominio di accesso sono: Microsoft 365, verrà integrato inoltre ogni nuovo applicativo, verrà invece effettuata un'analisi dei rischi per gli applicativi esistenti non integrati con particolare riferimento a quelli di prossima sostituzione.

ART 48) GESTIONE DEI DIRITTI DI ACCESSO

1. Devono essere definiti specifici profili di autorizzazione per l'accesso alle informazioni, da parte degli utenti del sistema informatico della ACSS (personale, nonché soggetti terzi ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali).
2. I profili di autorizzazione di cui al comma precedente devono consentire di individuare a quali informazioni l'utente può accedere nonché quali azioni può compiere. Al riguardo, le elaborazioni/operazioni autorizzate devono essere limitate a quelle strettamente necessarie allo svolgimento delle mansioni assegnate e nell'ambito di operatività definito, conformemente al principio del "need to know/need to do" e del "at least privilege". In

particolare, ai soggetti terzi deve essere consentito l'accesso alle informazioni della ACSS solo ed esclusivamente in funzione del proprio incarico.

3. Devono essere definite procedure di gestione e controllo del ciclo di vita dei profili di autorizzazione degli utenti del sistema informatico della ACSS (assegnazione, creazione, aggiornamento, disattivazione e revoca), inclusi i profili ad elevati privilegi.
4. Devono essere adottati controlli e procedure di sicurezza in grado di revocare, possibilmente tramite automatismi, i diritti di accesso degli utenti del sistema informatico della ACSS.

ART 49) RESPONSABILITÀ DELL'UTENTE

1. Devono essere definite idonee istruzioni per rendere edotti gli utenti sulle regole di sicurezza da attuare in merito alla scelta ed all'utilizzo delle password e sulle cautele per assicurarne la segretezza.
2. Tali istruzioni devono, altresì, definire le modalità per il corretto utilizzo delle postazioni di lavoro e degli strumenti informatici e telematici.
3. Il personale e gli eventuali soggetti terzi, ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali, devono essere informati delle conseguenze, disciplinari e anche giuridiche, derivanti dalla mancata applicazione/violazione (volontaria o involontaria) delle istruzioni ricevute.

ART 50) ACCESSO ALLA RETE E RELATIVI SERVIZI

1. L'accesso alla rete ed ai servizi di rete deve essere consentito solo al personale autorizzato nonché ai soggetti terzi ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.
2. In particolare, è carico del gestore della connettività di concerto con il responsabile della sicurezza delle informazioni di ACSS:
 - a. Il monitoraggio degli accessi in conformità alle normative vigenti e regolarmente verificati;
 - b. L'adozione di appropriati sistemi di autenticazione per il controllo degli accessi remoti alla rete;
 - c. Il controllo per gli accessi fisici e logici per la diagnostica e la configurazione delle porte;
 - d. L'attuazione di idonei controlli atti ad impedire l'accesso alla rete da parte di utenti non autorizzati.

- e. Presso ACSS devono essere attive connessioni VPN o disattivarle non appena possibile, riducendo al minimo i disagi per gli utenti interni.
- f. L'accesso alla rete Internet dalla sede di ACSS avviene tramite proxy (indirizzo: reglomb.proxy – porta 8080). L'accesso alla rete WI-FI avviene in automatico sulle postazioni di lavoro di tramite la rete avente SID ACSSWIFI dopo aver inserito l'apposita password fornita dal gestore della connettività e richi. Per i collaboratori esterni all'organizzazione l'accesso alla rete Internet tramite WIFI Consulenti@RL può essere concesso tramite apposite credenziali di durata annuale. Per l'accesso degli ospiti alla rete Internet è disponibile una rete pubblica a registrazione autonoma Guest@RL con credenziali a scadenza illimitata ma con utilizzo giornaliero limitato. Tali modalità di accesso fanno riferimento a quanto riportato nel Decreto di Regione Lombardia n. 13455 del 22 settembre 2022 – Regole per i Servizi Infotelematici della giunta regionale.

ART 51) ACCESSI AL SISTEMA OPERATIVO ED AL SOFTWARE DI BASE

- 1. L'accesso ai sistemi operativi ed al software di base deve essere controllato da un'ideale procedura di sicurezza (es. Accesso esclusivo tramite credenziali AD).
- 2. L'accesso al sistema operativo ed al software di base deve essere consentito solo al personale autorizzato nonché ai soggetti terzi ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.
- 3. Gli accessi devono essere monitorati e periodicamente verificati con cadenza temporale prestabilita, in conformità alle normative vigenti, e regolarmente verificati.
- 4. Devono essere definite procedure atte ad assicurare la creazione di codici per l'identificazione univoca utenti (user-id).
- 5. Il sistema deve essere configurato in modo da prevedere la chiusura automatica della sessione lavorativa dopo un periodo predefinito di inattività e la riattivazione della stessa solo previa autenticazione informatica.

ART 52) ACCESSI AI SISTEMI ED ALLE APPLICAZIONI

- 1. L'accesso ai sistemi ed alle applicazioni deve essere controllato da una ideale procedura di sicurezza e limitato al solo personale autorizzato nonché ai soggetti terzi cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.
- 2. Per l'accesso ai sistemi ed alle applicazioni che rivestono particolare criticità è opportuno che l'identificazione avvenga tramite meccanismi di autenticazione forte, la cui robustezza sia proporzionata al livello di criticità dei dati ivi contenuti.

3. Gli accessi ai sistemi ed alle applicazioni devono essere monitorati e regolarmente verificati, nel rispetto della normativa vigente.
4. Devono essere definite idonee procedure e controlli di sicurezza per proteggere i sistemi e le applicazioni dai rischi derivanti dall'utilizzo di computer portatili.
5. Nel caso in cui si utilizzino soluzioni per il lavoro da remoto devono essere definite ed attuate specifiche politiche e procedure per l'accesso in sicurezza ai sistemi ed alle applicazioni.
6. Nell'ambito del sistema di videoconferenza di ACSS, si rammenta la possibilità di usare diverse piattaforme (Webex, Teams, Zoom, ecc.) presso la postazione di lavoro installata nella sala riunioni. L'organizzazione di una riunione con la soluzione Webex richiede di:
 - Verificare la disponibilità della Sala (tramite il calendario già condiviso e gestito dai dirigenti e dalla segreteria della direzione);
 - Chiamare il numero 25000 chiedendo di pianificare la riunione comunicando i seguenti dati: Titolo, indirizzi mail dei partecipanti, data e ora di inizio, durata stimata;

I tecnici garantiscono l'assistenza necessaria per tutta la durata della riunione. Per utilizzare la soluzione Webex non dovrà essere attuata alcuna altra azione. Qualora fosse necessario condividere lo schermo potrà essere utilizzata la postazione di lavoro già presente oppure utilizzare un'altra postazione di lavoro (portatile) scollegando e collegando solo e solamente il cavo HDMI alla postazione di lavoro "aggiuntiva".

Qualora si voglia organizzare una riunione con la soluzione Teams (sistema facente parte della fornitura Microsoft 365 di ACSS) risulta necessario effettuare le seguenti azioni:

- Verificare la disponibilità della Sala (tramite il calendario già condiviso e gestito dai dirigenti e dalla segreteria della direzione);
- Pianificare autonomamente la riunione Teams.

Per utilizzare la soluzione Teams o Zoom (solo se pianificate da terzi) non dovrà essere attuata alcuna azione, è sufficiente impostare come periferiche la videocamera USB e il microfono d'ambiente esterni, qualora fosse necessario condividere lo schermo potrà essere utilizzata la postazione di lavoro già presente oppure utilizzare un'altra postazione di lavoro (portatile) scollegando e collegando solo e solamente il cavo HDMI alla postazione di lavoro "aggiuntiva" lasciando attiva la sessione di collegamento sulla postazione della sala.

15.ACQUISIZIONE, SVILUPPO E MANUTENZIONE

ART 53) ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI

1. L'acquisizione, lo sviluppo e la manutenzione dei sistemi della ACSS deve garantire la protezione delle informazioni da errori, perdite, modifiche non autorizzate o alterazioni.

ART 54) REQUISITI DI SICUREZZA DEI SISTEMI INFORMATIVI

1. La sicurezza deve essere parte integrante dei sistemi informativi utilizzati per la gestione delle informazioni della ACSS.
2. L'acquisizione di nuovi sistemi o di parti di sistemi esistenti deve includere, in accordo con i requisiti derivanti dagli scopi istituzionali e dalle politiche di sicurezza, la definizione di specifici requisiti e controlli di sicurezza.
3. Devono essere definiti specifici requisiti per l'identificazione e l'implementazione di appropriati controlli atti ad assicurare l'autenticità e l'integrità dei messaggi tra le applicazioni.

ART 55) SICUREZZA NEI PROCESSI DI SVILUPPO E SUPPORTO

1. Le applicazioni, sia commerciali che sviluppate appositamente per la ACSS, devono rispettare le politiche e le linee guida di sviluppo sicuro derivanti dagli standard e dalle best practice applicabili.
2. Le applicazioni devono essere protette in modo da impedire errori, perdite, modifiche non autorizzate o alterazioni non autorizzate delle informazioni.
3. Inoltre, qualora possibile, devono essere previsti controlli di congruità delle informazioni, incorporati all'interno delle applicazioni, per rilevare eventuali alterazioni delle medesime derivanti da errori di processo o da azioni deliberate.
4. Per i processi critici devono essere previste procedure per la validazione dei dati inseriti all'interno delle applicazioni al fine di garantire che il dato sia corretto ed appropriato.
5. L'installazione del sistema operativo e dei software di base (middleware, application server, database, ecc.) deve essere controllata e verificata attraverso la predisposizione di idonee procedure di test.
6. Tutte le modifiche apportate ai sistemi devono essere controllate.

7. Qualora siano previste delle modifiche al sistema operativo, le applicazioni critiche devono essere controllate e verificate tramite test, al fine di scongiurare eventuali malfunzionamenti dell'operatività e della sicurezza della ACSS.
8. Le modifiche ai pacchetti software devono essere limitate allo stretto necessario e, qualora effettuate, strettamente controllate.
9. Devono essere definite idonee procedure per il tracciamento delle modifiche e la successiva verifica.
10. Devono essere definite idonee procedure per la protezione degli ambienti utilizzati per lo sviluppo di nuove applicazioni o per le iniziative di integrazione, in termini di protezione delle informazioni, separazione degli ambienti di sviluppo, test, produzione e specifiche politiche di controllo accesso.
11. Per l'esecuzione dei test, non devono essere utilizzati dati personali ai sensi del GDPR o dati critici per l'ACSS. Qualora fosse strettamente necessario utilizzare i suddetti dati, occorre adottare tecniche di mascheramento o soluzioni similari.
12. I risultati del test devono essere controllati e conservati.

ART 56) SICUREZZA NELLA MANUTENZIONE

1. Devono essere adottate procedure ed istruzioni operative per la regolamentazione delle attività di manutenzione dei sistemi informativi. Le procedure devono definire:
 - a. i criteri e le modalità per l'aggiornamento periodico dei prodotti utilizzati;
 - b. la pianificazione e l'attuazione di interventi di manutenzione programmata (dismissione, sostituzione, ecc.);
 - c. il collaudo dell'operatività dei sistemi dopo gli interventi di aggiornamento e manutenzione;
 - d. l'aggiornamento della configurazione del sistema in funzione delle modifiche apportate all'ambiente.
2. Tutte le attività di manutenzione devono essere tracciate e regolarmente verificate.

Il gestore delle postazioni di lavoro adotta un manuale di servizio con indicate le politiche di governo della manutenzione in aderenza alle indicazioni fornite dal Regolamento Cybersecurity di ACSS.

16.GESTIONE DEGLI INCIDENTI RILEVANTI AI FINI DELLA SICUREZZA

ART 57) GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI E DEI MIGLIORAMENTI

1. Devono essere identificati, classificati e gestiti, in accordo con le normative nazionali ed interne alla ACSS, gli incidenti rilevanti ai fini della sicurezza delle informazioni.
2. Devono essere definite procedure per la gestione degli incidenti rilevanti ai fini della sicurezza delle informazioni in conformità alle vigenti normative nazionali e interne alla ACSS ed ai Service Level Agreement (SLA) previsti per i servizi erogati.
3. Tali procedure devono descrivere:
 - a. le modalità di monitoraggio, rilevamento e classificazione degli eventi di sicurezza, anche in relazione a quanto richiesto dalle normative applicabili in materia;
 - b. le modalità di gestione degli eventi rilevati e le procedure di escalation verso i soggetti interni ed esterni alla ACSS;
 - c. le finalità, le modalità, i criteri di protezione, di utilizzo ed i tempi di conservazione dei log rilevanti ai fini della ricostruzione delle cause di incidente;
 - d. La pianificazione e la verifica della risposta e del ripristino a seguito di un incidente devono essere condotti anche con i soggetti terzi, in relazione alle attività da questi svolte in forza degli accordi contrattuali.
4. Tutto il personale della ACSS e i soggetti terzi devono attenersi alle indicazioni ricevute in materia di sicurezza delle informazioni e contenute nelle istruzioni operative di riferimento, che devono essere opportunamente redatte.
5. Tutto il personale della ACSS e i soggetti terzi che individuano o abbiano il sospetto riguardante un incidente di sicurezza, devono segnalarlo immediatamente secondo le modalità appositamente stabilite allo scopo.
6. Devono essere previste sanzioni disciplinari in caso di violazione dei vincoli di sicurezza da parte del personale, in accordo con quanto previsto dalle norme contrattuali vigenti.
7. Devono essere, altresì, previste sanzioni in caso di violazione dei vincoli di sicurezza da parte dei soggetti terzi che accedono ed utilizzano le Risorse Informative per l'esecuzione degli specifici obblighi contrattuali.

17.GESTIONE DELLA CONTINUITÀ OPERATIVA

ART 58) ASPETTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI NELLA GESTIONE DELLA CONTINUITÀ OPERATIVA

1. Deve essere garantita la continuità operativa della ACSS, con l'obiettivo di ripristinare una situazione di normalità entro un tempo prestabilito (in funzione dei livelli di servizio attesi), minimizzando gli impatti sui servizi erogati dall'Amministrazione, derivanti dall'interruzione delle attività a fronte di un incidente di sicurezza, un guasto o disastro.
2. Il requisito di resilienza per ACSS consiste nel poter disporre di una connettività ridondata presso la sede di lavoro e della disponibilità immediata di altra postazione di lavoro opportunamente configurata in caso di guasto della postazione in dotazione. Il gestore della connettività e il gestore delle postazioni di lavoro garantiscono tali aspetti in aderenza agli SLA previsti dal contratto.

18. CONTROLLI DI CONFORMITÀ

ART 59) CONFORMITÀ AI REQUISITI DI SICUREZZA

1. La conformità ai requisiti di sicurezza definiti dalle normative cogenti, dagli standard internazionali e dalle best practice applicabili alla ACSS, risulta imprescindibile nell'ambito del raggiungimento degli obiettivi di sicurezza espressi dalla Politica della Sicurezza delle Informazioni.
2. Tali requisiti sono presi in considerazione nell'ambito della definizione delle direttive esplicitate negli Statement che indirizzano la tutela delle Risorse Informative della ACSS.

19.CONFORMITÀ AI REQUISITI COGENTI E CONTRATTUALI

ART 60) NORMATIVA GENERALE IN MATERIA DI SICUREZZA DELLE INFORMAZIONI

1. La ACSS deve prevedere un processo di analisi periodica della normativa generale in materia di sicurezza delle informazioni applicabile alla ACSS e attuare le attività necessarie per garantire la conformità a tale normativa.

2. In particolare, la ACSS, nell'ambito della definizione delle strategie di gestione della sicurezza delle informazioni, deve ottemperare ai requisiti derivanti dai principi generali enunciati dall'attuale legislazione italiana ed europea inerente, a titolo esemplificativo e non esaustivo, alle seguenti tematiche:
 - a. Infrastrutture critiche e cybersecurity;
 - b. Criminalità informatica;
 - c. Tutela del trattamento dei dati personali;
 - d. Tutela del software e delle banche dati;
 - e. Responsabilità amministrativa e penale a carico di amministratori e dirigenti;
 - f. Validità giuridica del documento informatico;
 - g. Contratto Collettivo Nazionale di Lavoro e sue integrazioni.

ART 61) NORMATIVA SPECIFICA E DI SETTORE APPLICABILE AI SERVIZI DELLA ACSS

1. La ACSS deve prevedere un processo di analisi periodica della normativa specifica e di settore in materia di sicurezza ICT applicabile ai servizi istituzionali erogati dalla ACSS e attuare le attività necessarie per garantire la conformità a tale normativa.

ART 62) REQUISITI CONTRATTUALI

1. La ACSS deve documentare e mantenere aggiornati tutti i requisiti contrattuali inerenti alla sicurezza delle informazioni e attuare le attività necessarie per garantire la conformità a tali requisiti.

20.CONFORMITÀ A STANDARD INTERNAZIONALI E BEST PRACTICES

ART 63) STANDARD INTERNAZIONALI E BEST PRACTICE

1. La ACSS deve adottare un approccio metodologico, per la gestione delle problematiche inerenti alla sicurezza delle informazioni, conforme agli standard internazionali ed alle best practice nazionali ed internazionali di riferimento per la definizione di ruoli, responsabilità, procedure formali di gestione dei processi legati alla sicurezza, sia per l'operatività della ACSS, sia per il trattamento delle emergenze.
2. A tal riguardo occorre prevedere un processo di analisi periodica degli standard internazionali e best practice inerenti alla sicurezza delle informazioni applicabili alla ACSS, tra questi identificare quelli più idonei in relazione al contesto della ACSS e attuare le attività necessarie per recepirli nel contesto organizzativo.

21. RIESAME DELLA SICUREZZA DELLE INFORMAZIONI

ART 64) VERIFICA E RIESAME DELLA SICUREZZA DELLE INFORMAZIONI

1. Devono essere effettuate attività di verifica e riesame, al fine di assicurare che la sicurezza delle informazioni sia attuata e gestita in conformità alle politiche ed alle procedure della ACSS.
2. La ACSS deve effettuare, con periodicità predefinita e in occasione di cambiamenti significativi, un riesame indipendente dell'approccio definito per la sicurezza delle informazioni in termini di obiettivi, controlli, politiche, processi e procedure.
3. Deve inoltre essere riesaminata regolarmente la conformità dei processi inerenti alla sicurezza delle informazioni attuati presso la ACSS rispetto alle politiche, alle norme e a ogni altro requisito appropriato per la sicurezza.
4. Infine, devono essere effettuate regolarmente verifiche tecniche dei sistemi informativi al fine di verificarne la conformità rispetto alle politiche e alle norme per la sicurezza delle informazioni.

22. IL SISTEMA DOCUMENTALE

ART 65) SISTEMA DOCUMENTALE PER LA SICUREZZA DELLE INFORMAZIONI

1. Il raggiungimento degli obiettivi di protezione delle Risorse Informative della ACSS e l'attuazione controlli definiti nel presente documento (cfr. Titolo V e Titolo VI), presuppone la creazione di un adeguato sistema documentale.
2. La ACSS ha definito e strutturato il sistema documentale specifico inerente alla sicurezza delle informazioni che consente di indirizzare il governo delle problematiche relative alla protezione delle Risorse Informative. A partire dalla presente politica, tale sistema si sostanzia in Politiche generali e specifiche per la Sicurezza delle Informazioni, Linee Guida, Procedure e Istruzioni operative, secondo il seguente schema:
 - a. **Politica per la sicurezza delle Informazioni:** documento (il presente) che fornisce una serie di principi, modalità di azione, requisiti organizzativi, di alto livello e non derogabili, finalizzata a definire l'ambito di applicazione e a guidare il governo della sicurezza delle informazioni, in linea con le volontà dell'Alta Direzione;

- b. **Politiche generali per la Sicurezza delle Informazioni:** documentazione che fornisce regole inderogabili di alto livello su temi generali inerenti alla sicurezza delle informazioni, derivati dalla suddetta Politica per la sicurezza delle Informazioni;
 - c. **Politiche Specifiche per la Sicurezza delle Informazioni:** documentazione che fornisce regole inderogabili di alto livello su temi specifici di sicurezza delle informazioni;
 - d. **Linee Guida:** documentazione che fornisce raccomandazioni, a carattere generale o specifico, derogabili e la cui implementazione è rimessa alle figure responsabili dei servizi/processi/applicazione. In caso di deroga, le suddette figure devono documentare le ragioni della non aderenza alle linee guida e le scelte effettuate in alternativa;
 - e. **Procedure operative:** documentazione che descrive le modalità operative (chi, cosa, come, quando, dove) nell'ambito dei processi di sicurezza e dei controlli implementati per l'attuazione delle Politiche e delle Linee Guida;
 - f. **Istruzioni operative:** documentazione descrittiva dei compiti e delle attività effettuate dal personale operativo.
3. Le Politiche, le Linee Guida, le Procedure e le Istruzioni Operative devono essere strutturate in modo semplice e comprensibile al personale di ogni livello organizzativo. Tale documentazione deve essere pubblicata, resa disponibile a tutti i soggetti interessati e revisionata periodicamente.

23.DOCUMENTI DI RIFERIMENTO

1. Regolamento UE n. 679/2016 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE – General Data Protection Regulation (GDPR).
2. D.lgs. 101/2018: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
3. Deliberazione del Garante Privacy numero 53 del 23 novembre 2006: Linee guida in materia di trattamento di dati personali di lavoratori.
4. Deliberazione del Garante Privacy numero 13 del 1° marzo 2007: Uso delle e-mail e di Internet.
5. Provvedimento del Garante Privacy del 13 ottobre 2008: Smaltimento e cancellazione sicura dei dati.

6. Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori - Scheda informativa del Garante per la protezione dei dati personali del 12 dicembre 2008.
7. Provvedimento del Garante Privacy dell'8 aprile 2010: Videosorveglianza.
8. Provvedimento del Garante Privacy: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27 novembre 2008 e successive modifiche e integrazioni.
9. Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS).
10. D.lgs. 65/2018: Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" (Attuazione Direttiva (UE) NIS 2016/1148) aggiornato dal Decreto-Legge 14 giugno 2021, n. 82.
11. Linee Guida per gli Operatori di Servizi Essenziali – Autorità NIS-Settore Salute – luglio 2019.
12. Direttiva 2009/136/CE, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.
13. "Linee guida in materia di Dossier sanitario" del Garante per la protezione dei dati personali del 4 giugno 2015 (G.U. n. 164 del 17 luglio 2015).
14. D.lgs. 105/2019: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.
15. PIANO NAZIONALE DI RIPRESA E RESILIENZA, #NEXTGENERATIONITALIA, Italia Domani.
16. DPCM 14 aprile 2021, n. 81. Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.
17. Decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.
18. Framework Nazionale per la Cybersecurity e la Data Protection.
19. ISO 9001:2008: Sistemi di Gestione per la Qualità – Requisiti.
20. ISO/IEC 73:2009: Risk management – Vocabulary – Guidelines for use in standards.
21. UNI ISO 31000: 2010: Gestione del rischio – Principi e linee guida.
22. ISO/IEC 27001: Tecnologie Informatiche - Tecniche per la Sicurezza - Sistemi di Gestione per la Sicurezza delle Informazioni – Requisiti.
23. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.
24. ISO/IEC 27003: Information Technology – Security Techniques – Information security management system implementation guidance.

-
25. ISO/IEC 27004: Information Technology – Security Techniques – Information security management – Measurement.
 26. ISO/IEC 27005: Information Technology – Security Techniques – Information security risk management.
 27. D.lgs. n. 82/2005: Codice dell'amministrazione digitale e successive modificazioni e integrazioni.
 28. Misure minime di sicurezza per le PA, AgID.
 29. Determinazione n. 220/2020 del 17 maggio 2020 - Adozione delle Linee Guida – La sicurezza nel procurement ICT, AgID.
 30. Decreto del Direttore Della Repubblica 16 aprile 2013, n. 62: Regolamento recante codice di comportamento dei dipendenti pubblici.
 31. Regolamento (UE) 2019/881 (Cybersecurity act) del 17 aprile 2019.
 32. Decreto Legislativo 3 aprile 2006, n. 152 - Norme in materia ambientale.
 33. LEGGE 20 maggio 1970, n. 300 (Statuto dei lavoratori).
 34. Regolamento per i procedimenti disciplinari relativi al personale dipendente del comparto della dirigenza della ACSS.

RUOLI E RESPONSABILITÀ PER LA SICUREZZA DELLE INFORMAZIONI

L'ACSS ha adottato un approccio sistematico alla cybersecurity e più in generale alla sicurezza delle informazioni che indirizza un insieme organico e strutturato di misure di sicurezza logica, fisica, organizzativa e procedurale dedicate alla protezione dell'integrità, della riservatezza e della disponibilità delle informazioni e delle reti di comunicazione, declinato in una *Politica per la Sicurezza delle Informazioni*.

Per dare attuazione a quanto definito nella suddetta Politica si è dotata di un modello organizzativo per la sicurezza delle informazioni che si concretizza nella definizione di ruoli, funzioni e responsabilità che concorrono alla realizzazione ed alla gestione del *sistema di sicurezza delle informazioni*, tenendo conto anche del ruolo della ACSS nel settore di riferimento e all'interno della filiera produttiva. Sebbene la realtà della ACSS sia di modeste dimensioni e non siano presenti alcune articolazioni organizzative "tipiche" di realtà più complesse, si riportano tutti i ruoli previsti anche se alcuni possano essere internamente ricoperti dal medesimo dipendente e altri siano demandati a soggetti esterni nell'ambito di convezioni attuate da ACSS.

1. INTRODUZIONE

ART 1) SCOPO DEL DOCUMENTO

1. Il presente documento descrive i ruoli coinvolti nella gestione della sicurezza delle informazioni e le annesse responsabilità, conformemente a quanto previsto nella *Politica per la Sicurezza delle Informazioni della ACSS*, nonché le relazioni tra tali ruoli e gli uffici/funzioni organizzative della ACSS.

ART 2) CAMPO DI APPLICAZIONE

1. I contenuti del presente documento sono validi per l'intera ACSS.

ART 3) DEFINIZIONI E ACRONIMI

1. Ai fini dell'applicazione del presente documento devono intendersi le seguenti definizioni:
 - a. **Autorità nazionale competente NIS**: autorità nazionale unica, competente in materia di sicurezza delle reti e dei sistemi informativi, di cui all'articolo 7, comma 1 del decreto legislativo 18 maggio 2018, n.65.
 - b. **Cybersecurity**: l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni

- elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza.
- c. **CSIRT Italia**: il Computer Security Incident Response Team, di cui all'articolo 8 del decreto legislativo NIS.
 - d. **Direttiva NIS** : Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, recepita in Italia con il decreto legislativo 18 maggio 2018, n.65.
 - e. **Risorse Informative**: cfr. Art. 2).
2. Ai fini dell'applicazione del presente documento devono intendersi i seguenti acronimi:
- a. **ACN**: Agenzia per la cybersicurezza nazionale.
 - b. **ACSS**: Agenzia di Controllo del Sistema Sociosanitario lombardo.
 - c. **CSIRT**: Computer Security Incident Response Team.
 - d. **NIS**: Network and Information Security.

2. RUOLI COINVOLTI NELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

ART 4) DIRETTORE GENERALE DELLA ACSS

1. Il *Direttore Generale* della ACSS è il responsabile delle politiche per la sicurezza delle informazioni della ACSS e dei relativi ruoli e responsabilità, della loro emanazione, attuazione ed aggiornamento anche in ottica di miglioramento continuo.
2. Il *Direttore Generale* della ACSS si avvale del supporto tecnico ed organizzativo del Responsabile ICT, del Responsabile della Sicurezza delle Informazioni, del Responsabile della Transizione Digitale, del Comitato Direttivo per la Sicurezza delle Informazioni e del DPO.
3. Il *Direttore Generale* della ACSS è responsabile di garantire la continuità operativa della ACSS.

ART 5) COMITATO DIRETTIVO PER LA SICUREZZA DELLE INFORMAZIONI (CDSI)

1. Il *CDSI* è l'organo decisionale in termini di politiche ed investimenti da sostenere per la sicurezza delle informazioni della ACSS.
2. Il *CDSI* ha la funzione di supportare il *Direttore Generale* della ACSS nella ricerca ed indicazione delle linee guida e delle migliori modalità di applicazione delle politiche per la sicurezza delle informazioni, anche in ottica di miglioramento continuo.
3. Il *CDSI* è costituito dai seguenti ruoli:
 - a. *Direttore Generale della ACSS*;

- b. *Responsabile della protezione dei dati personali (DPO);*
 - c. *Responsabile delle Risorse Umane per la sicurezza delle informazioni;*
 - d. *Responsabile degli Approvvigionamenti per la sicurezza delle informazioni;*
 - e. *Responsabile ICT;*
 - f. *Responsabile della Sicurezza delle Informazioni;*
 - g. *Responsabile della Safety e della Sicurezza Fisica;*
 - h. *Responsabile delle Facilities;*
 - i. *Referente NIS.*
4. Il *Direttore Generale* della ACSS può scegliere e convocare i membri del *CDSI* garantendo l'adeguatezza della composizione in riferimento agli ambiti e le problematiche del caso. Inoltre, in relazione a tematiche specifiche, il *Direttore Generale* della ACSS può estendere la partecipazione alle riunioni del *CDSI* anche ad altre figure della ACSS.
5. Il *CDSI* si riunisce normalmente con cadenza semestrale. Tuttavia, su richiesta del *Direttore Generale* della ACSS, può essere convocato "ad evento" e/o con una frequenza superiore a quella semestrale.
6. Il *CDSI* approva le deroghe a:
- a. le regole riportate nelle politiche per la sicurezza delle informazioni della ACSS, solo nei casi in cui ne sia valutato ed accettato il rischio cyber derivante garantendone la comunicazione ai soggetti interessati ai fini della loro attuazione;
 - b. la soglia di accettazione del rischio definita dalla ACSS nella *Politica per la Sicurezza delle Informazioni*, nell'ambito delle specifiche analisi del rischio cyber su servizi o applicazioni e solo per comprovate esigenze garantendone la comunicazione ai soggetti interessati ai fini della loro attuazione.
7. Al *CDSI* è assegnata la responsabilità decisionale e la supervisione delle attività e delle risorse coinvolte nel sistema di gestione della continuità operativa, al verificarsi di situazioni di emergenza ICT.

ART 6) RESPONSABILE DELLE RISORSE UMANE PER LA SICUREZZA DELLE INFORMAZIONI

1. Il *Responsabile delle Risorse Umane per la sicurezza delle informazioni* ha la responsabilità di:
- a. individuare attentamente i *Dipendenti e assimilabili* e i *Soggetti terzi* destinati a ricoprire ruoli di gestione della sicurezza, in funzione delle esigenze istituzionali della ACSS e sulla base di criteri di affidabilità e competenza professionale;
 - b. assegnare, dopo l'individuazione, ai *Dipendenti e assimilabili* dedicati alla sicurezza delle informazioni, oltre alla struttura organizzativa di appartenenza, anche specifici ruoli operativi e profili professionali, previo adeguato percorso formativo ad hoc;

- c. informare i *Dipendenti e assimilabili* delle responsabilità e doveri in materia di sicurezza delle informazioni della ACSS con riferimento all'intera durata del rapporto di lavoro ed alla sua variazione/cessazione.
2. Il *Responsabile delle Risorse Umane per la sicurezza delle informazioni* ha inoltre la responsabilità di assicurare che i cambiamenti organizzativi e delle mansioni assegnate ai *Dipendenti e assimilabili* che comportano variazioni del profilo d'accesso ai sistemi, applicazioni e dati, siano comunicati ai suddetti interessati, al *Responsabile della Struttura/Ufficio* di competenza e al *Responsabile ICT*, affinché quest'ultimo possa variare o, se necessario, revocare il profilo e le credenziali di accesso.

ART 7) RESPONSABILE DEGLI APPROVVIGIONAMENTI PER LA SICUREZZA DELLE INFORMAZIONI

1. Il *Responsabile degli Approvvigionamenti per la sicurezza delle informazioni* ha la responsabilità di definire ed attuare per quanto di propria competenza e con il supporto del Responsabile ICT e della Sicurezza delle Informazioni, le procedure per garantire la sicurezza delle informazioni in relazione all'approvvigionamento di beni e servizi che indirizzino tutte le fasi di approvvigionamento (prima, durante e dopo). Le procedure devono altresì contemplare:
 - a. la predisposizione di specifiche clausole per garantire la riservatezza delle informazioni e la protezione delle Risorse Informative della ACSS accedute ed utilizzate dai *Soggetti terzi*, secondo quanto previsto dalle normative vigenti, indirizzando l'intera catena di approvvigionamento a garanzia del mantenimento della sicurezza delle informazioni in tutte le fasi. Tali clausole sono predisposte con il supporto del *Responsabile della Sicurezza delle Informazioni* e del *Responsabile ICT*;
 - b. la comunicazione ai *Soggetti terzi* delle politiche, procedure e istruzioni di sicurezza della ACSS applicabili al tipo di attività previste dal contratto.

ART 8) RESPONSABILE DELLA SICUREZZA DELLE INFORMAZIONI

1. Il *Responsabile della Sicurezza delle Informazioni* ha la responsabilità di:
 - a. sovrintendere alla realizzazione della "struttura di sicurezza della ACSS", in termini di organizzazione, politiche, linee guida, processi ed eventuali procedure e baseline di sicurezza, finalizzata a prevenire e proteggere, in armonia con le misure stabilite, il complesso degli archivi, delle procedure e dei sistemi, da minacce ed eventi critici, anche con riferimento ai rapporti con i *Soggetti terzi*;
 - b. definire politiche, linee guida, processi ed eventuali procedure e baseline di sicurezza, di valenza generale;
 - c. contribuire alla formazione e sensibilizzazione del personale *Dipendente o assimilabile* e degli eventuali *Soggetti terzi* sulle politiche, linee guida e procedure relative alla sicurezza delle informazioni;

- d. effettuare l'analisi e la gestione dei rischi cyber congiuntamente al *Responsabile di Dipartimento/Struttura* con il supporto del *Responsabile delle Facilities*, del *Responsabile della Safety e della Sicurezza Fisica*, del *Responsabile ICT* (qualora non coincidente con il Responsabile della Sicurezza delle Informazioni) sulla base delle rispettive competenze ed effettuare il coordinamento delle relative attività;
- e. svolgere attività di verifica finalizzate a fornire idonea garanzia;
- f. del pieno rispetto delle disposizioni, anche legislative, vigenti in materia di sicurezza dell'informazione e dei vincoli derivanti da obblighi contrattuali;
- g. della conformità delle procedure/istruzioni operative che disciplinano tematiche specifiche alle politiche, linee guida, processi, procedure e baseline di sicurezza, di valenza generale;
- h. della conformità delle attività eseguite alle politiche/procedure definiti dalla ACSS e ai requisiti di sicurezza scaturiti dall'Analisi dei rischi cyber e di quelli inerenti alla catena di approvvigionamento cyber;
- i. predisporre e mantenere aggiornata, con il supporto del *Referente NIS*, del *DPO*, del *Responsabile delle Facilities*, del *Responsabile della Safety e della Sicurezza Fisica*, del *Responsabile ICT*, la mappatura delle misure tecniche e organizzative di sicurezza (assessment) in essere rispetto a quelle richieste dalla normativa NIS;
- j. supportare il *Responsabile degli Approvvigionamenti per la sicurezza delle informazioni* nella predisposizione di specifiche clausole per garantire la riservatezza delle informazioni e la protezione delle Risorse Informative della ACSS accedute ed utilizzate dai Soggetti terzi, secondo quanto previsto dalle normative vigenti;
- k. supportare il *Referente NIS* nel valutare, alla luce di tutti gli elementi disponibili, la rilevanza dell'impatto di un incidente e nel predisporre la relativa documentazione.

ART 9) RESPONSABILE DELLA SAFETY E DELLA SICUREZZA FISICA

1. L'ACSS non prevede la figura del *Responsabile della Safety e della Sicurezza Fisica* in quanto risulta in capo a soggetti terzi (Convenzione sugli spazi con la Giunta Regionale (Determinazione del Direttore dell'Agenzia n.119 del 21/12/2018 - "*Approvazione nuovo schema di Accordo per la concessione spazi nelle sedi istituzionali agli enti facenti parte del Sistema regionale ai sensi della LR 30/2006 e partecipate*") lo sviluppo, implementazione e gestione delle misure per la sicurezza delle informazioni inerenti alla Sicurezza Fisica e Ambientale, con particolare riferimento ai seguenti ambiti:
 - a. sicurezza delle aree, incluse quelle sensibili;
 - b. controllo degli accessi fisici;
 - c. sicurezza degli uffici, delle stanze e degli strumenti di lavoro;
 - d. sicurezza delle aree di carico e scarico;
 - e. sicurezza del cablaggio.

ART 10) RESPONSABILE DELLE FACILITIES

1. L'ACSS non prevede la figura del *Responsabile delle Facilities a Safety e della Sicurezza Fisica* in quanto risultano in capo a soggetti terzi (Convenzione sugli spazi con la Giunta Regionale - Determinazione del Direttore dell'Agenzia n. 119 del 21/12/2018) lo sviluppo, implementazione e gestione delle misure per la sicurezza delle informazioni inerenti agli edifici e ai loro impianti (Facility management), con particolare riferimento all'equipaggiamento di sicurezza finalizzato alla protezione da minacce di tipo fisico ed ambientale (es. sistemi di controllo del livello di temperatura ambientale e di umidità, rilevazione incendio/allagamento, UPS – Sistemi Continuità elettrica).
2. Il *Responsabile delle Facilities* deve garantire per il proprio ambito di competenza, il rispetto di quanto previsto dalle politiche, linee guida, eventuali procedure e baseline definite dal *Responsabile della Sicurezza delle Informazioni*, anche con riferimento ai rapporti con i *Soggetti terzi*.

ART 11) RESPONSABILE ICT

1. Il *Responsabile ICT* è responsabile dello sviluppo, implementazione e gestione delle misure per la sicurezza delle informazioni inerenti ai sistemi e alle infrastrutture ICT e alle relative attività operative.
2. Il *Responsabile ICT*, deve garantire per il proprio ambito di competenza, il rispetto di quanto previsto dalle politiche, linee guida, eventuali procedure e baseline definite dal *Responsabile della Sicurezza delle Informazioni*, anche con riferimento ai rapporti con i *Soggetti terzi*.
3. Il *Responsabile ICT* predispone le procedure/istruzioni operative specifiche per gli ambiti di competenza.
4. Il *Responsabile ICT* è responsabile della verifica e del monitoraggio delle misure per la sicurezza delle informazioni di cui al precedente comma 1 del presente articolo, anche quando svolte da *Soggetti terzi*. Il *Responsabile ICT* è altresì responsabile della segnalazione delle eventuali non conformità rilevate, nonché del monitoraggio del rientro dalle suddette non conformità.
5. Il *Responsabile ICT* è responsabile inoltre di:
 - a. assicurare la pianificazione regolare e l'esecuzione di esercitazioni per verificare le reazioni dei sistemi ICT e del personale a supporto in caso di emergenza, la validità dei supporti e della documentazione di back up, nonché la capacità di ripristinare i sistemi entro il tempo necessario a garantire la continuità delle attività condotte dalla ACSS;

- b. coinvolgere il *Responsabile della Sicurezza delle Informazioni* per qualsiasi intervento che comporti impatti sulla sicurezza delle informazioni/sistemi/applicazioni;
 - c. monitorare e analizzare gli eventi di sicurezza ICT;
 - d. gestire gli incidenti di sicurezza ICT con il supporto, in base alla specifica competenza, del *Responsabile Facilities*, del *Responsabile della Safety e della Sicurezza Fisica* e del *Responsabile Tecnologie biomediche*;
 - e. supportare il *Responsabile degli Approvvigionamenti per la sicurezza delle informazioni* nella predisposizione di specifiche clausole per garantire la riservatezza delle informazioni e la protezione delle Risorse Informative della ACSS accedute ed utilizzate dai *Soggetti terzi*, secondo quanto previsto dalle normative vigenti;
 - f. supportare il *Responsabile della Sicurezza delle Informazioni* nel predisporre e mantenere aggiornata la mappatura delle misure tecniche e organizzative di sicurezza (assessment) in essere rispetto a quelle richieste dalla normativa NIS;
 - g. supportare il Direttore di S.C. alle informazioni in funzione del ruolo e delle funzioni ricoperte (chi può accedere a quali informazioni, come e quando);
 - h. supportare il *Referente NIS* (qualora previsto) nel valutare, alla luce di tutti gli elementi disponibili, la rilevanza dell'impatto di un incidente e nel predisporre la relativa documentazione.
6. Il *Responsabile ICT* partecipa per quanto di sua competenza a:
- a. il processo di valutazione del rischio cyber;
 - b. l'inventario degli asset;
 - c. il processo di gestione della continuità operativa.
7. Il *Responsabile ICT* assicura che ogni eventuale violazione delle misure di sicurezza afferenti al proprio ambito di competenza, sia denunciata alla struttura competente della ACSS, adottando un'ideale procedura.

ART 12) RESPONSABILE TECNOLOGIE BIOMEDICHE

1. Non previsto in ACSS.

ART 13) REFERENTE NIS

1. Non previsto in ACSS per quelli che sono i servizi esposti al cittadino alla data di redazione del seguente regolamento.

Il *Referente NIS* è responsabile, nell'ambito di applicabilità della Direttiva NIS, di:

- a. cooperare con l'Autorità nazionale competente NIS e fungere da punto di contatto per l'Autorità nazionale competente NIS per questioni connesse agli adempimenti previsti dalla Direttiva NIS;

- b. valutare, alla luce di tutti gli elementi disponibili, con il supporto del *Responsabile ICT* ed il *Responsabile della Sicurezza delle Informazioni*, la rilevanza dell'impatto di un incidente;
- c. predisporre, con il supporto del *Responsabile ICT* ed il *Responsabile della Sicurezza delle Informazioni*, tutta la documentazione inerente agli incidenti prevista dalle suddette Linee Guida;
- d. notificare al CSIRT Italia gli incidenti, senza ingiustificato ritardo, secondo le modalità in vigore all'atto della notifica;
- e. supportare il *Responsabile della Sicurezza delle Informazioni* nel predisporre e mantenere aggiornata la mappatura delle misure tecniche e organizzative di sicurezza (assessment) in essere rispetto a quelle richieste dalla normativa NIS.

2. Il *Responsabile NIS* ha inoltre la responsabilità di:

- a. predisporre le procedure/istruzioni operative specifiche per gli ambiti di competenza;
- b. coinvolgere il *Responsabile della Sicurezza delle Informazioni* per qualsiasi intervento che comporti impatti sulla sicurezza delle informazioni;

ART 14) VICARIO NIS

1. Non previsto in ACSS.

ART 15) RESPONSABILE DI DIREZIONE SANITARIA, SOCIO-SANITARIA E AMMINISTRATIVA

Non previsto in ACSS.

ART 16) RESPONSABILE DI STRUTTURA/UFFICIO

1. Il *Responsabile di Struttura/Ufficio*, per il proprio ambito di competenza, ha le seguenti responsabilità:
- a. definire formalmente, con il supporto del *Responsabile ICT*, il "profilo di accesso" degli utenti che accedono alle informazioni in funzione del ruolo e delle funzioni ricoperte (chi può accedere a quali informazioni, come e quando);
 - b. assicurare che ogni eventuale violazione delle misure di sicurezza che avviene sulle informazioni afferenti al proprio ambito di competenza, sia denunciata alla struttura competente della ACSS, adottando un'ideale procedura;
 - c. definire gli obiettivi e i requisiti di continuità operativa dei servizi di competenza;
 - d. classificare le informazioni afferenti al proprio ambito di competenza in funzione dei livelli di esposizione al rischio e delle politiche definite dalla ACSS;
 - e. eseguire l'analisi e la gestione dei rischi cyber congiuntamente al *Responsabile della Sicurezza delle Informazioni* e al *Responsabile ICT*;

- f. individuare le normative specifiche in materia di sicurezza ICT applicabili ai servizi istituzionali erogati e coinvolgere il *Responsabile della Sicurezza delle Informazioni* ai fini della definizione delle opportune modalità di attuazione;
 - g. deve garantire per il proprio ambito di competenza, il rispetto di quanto previsto dalle politiche, linee guida, eventuali procedure e baseline definite dal *Responsabile della Sicurezza delle Informazioni*.
- 2. Inoltre, Il *Responsabile di Struttura/Ufficio* ha la responsabilità di assicurare che i *Dipendenti e assimilabili* e i *Soggetti terzi* assegnati alla propria struttura/ufficio:
 - a. siano informati delle clausole di riservatezza contenute nel contratto di lavoro (es. il dipendente osserva il segreto professionale, segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali);
 - b. siano istruiti, anche tramite appositi corsi, da attivarsi a cura del *Responsabile della sicurezza delle informazioni* di concerto con il responsabile delle *Risorse Umane* circa la loro responsabilità rispetto alla sicurezza delle informazioni;
 - c. siano autorizzati all'accesso a sistemi o applicazioni o dati a seguito di individuazione del "profilo di accesso" coerentemente con il ruolo e le attività svolte. La comunicazione per l'autorizzazione dei diritti di accesso da inviare al *Responsabile ICT* deve essere effettuata nel rispetto delle procedure specifiche di accesso dei sistemi o applicazioni o dati;
 - d. siano addestrati all'uso delle risorse informative alle quali sono stati autorizzati;
 - e. abbiano preso conoscenza delle politiche di sicurezza delle informazioni della ACSS e delle procedure applicabili all'ambito di operatività;
 - f. siano autorizzati all'accesso ai locali della ACSS, coerentemente con il ruolo e le attività svolte, fornendo apposita comunicazione al *Responsabile della Safety e della Sicurezza Fisica*.
- 3. Il *Responsabile di Struttura/Ufficio* ha inoltre la responsabilità di assicurare che i cambiamenti delle attività svolte dai *Dipendenti e assimilabili* e dei *Soggetti terzi* assegnati alla propria struttura organizzativa che comportano variazioni del profilo d'accesso ai sistemi, applicazioni e dati, siano comunicati ai suddetti interessati e al *Responsabile ICT*, affinché quest'ultimo possa variare o, se necessario, revocare il profilo e le credenziali di accesso.
- 4. Il *Responsabile di Struttura/Ufficio* ha la responsabilità di assicurare che i cambiamenti delle attività svolte dai *Dipendenti e assimilabili* e dei *Soggetti terzi* assegnati alla propria struttura organizzativa che comportano variazioni dei diritti di accesso ai locali della ACSS siano comunicati ai suddetti interessati e al *Responsabile della Safety e della Sicurezza Fisica*, affinché quest'ultimo possa variare o, se necessario, revocare le autorizzazioni.

5. Il *Responsabile della Struttura/Ufficio* deve garantire per il proprio ambito di competenza, il rispetto di quanto previsto dalle politiche, linee guida, procedure e baseline definite dal *Responsabile della Sicurezza delle Informazioni*.
6. Il *Responsabile di Struttura/Ufficio* si interfaccia con il *Responsabile della Sicurezza delle Informazioni* per la corretta implementazione, all'interno della propria struttura/ufficio, delle politiche, linee guida, procedure e baseline definite da quest'ultimo.

ART 17) PERSONALE DIPENDENTE O ASSIMILABILE

1. Il personale *Dipendente o assimilabile*, nell'ambito delle proprie attività lavorative deve attenersi alle disposizioni della ACSS in materia di sicurezza delle informazioni ed alla stretta osservanza delle relative politiche e procedure applicabili, ivi compresa la segnalazione senza ritardo di ogni eventuale attività contraria alle suddette politiche/procedure, di cui venga a conoscenza.

ART 18) SOGGETTI TERZI

1. I *Soggetti terzi*, ossia i fornitori, consulenti, collaboratori esterni e partner che operano con la ACSS in forza di un contratto, nello svolgimento delle attività lavorative previste dai contratti in essere, devono attenersi alle disposizioni in materia di sicurezza delle informazioni della ACSS ed alla stretta osservanza delle relative politiche/procedure applicabili, ivi compresa la segnalazione senza ritardo di ogni eventuale attività contraria alle suddette politiche/procedure, di cui vengano a conoscenza.

3. FUNZIONI AZIENDALI COINVOLTE NELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

ART 19) CORRISPONDENZA TRA RUOLI COINVOLTI NELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI E FUNZIONI DELLA ACSS

1. I ruoli identificati nel presente regolamento sono attribuiti agli uffici/funzioni organizzative della ACSS come di seguito descritto:
 - Responsabile ICT: SC Analisi e Sviluppo Sistemi di Controllo
 - Responsabile per la Sicurezza delle Informazioni: SC Analisi e Sviluppo Sistemi di Controllo;
 - Responsabile delle Risorse Umane per la sicurezza delle informazioni: SC Giuridico e Risorse Umane;
 - Responsabile della protezione dei dati personali (DPO): soggetto individuato dal Direttore Generale;

- Responsabile degli Approvvigionamenti per la sicurezza delle informazioni: SS Risorse Strumentali
- Responsabile della Safety e della Sicurezza Fisica: Soggetto terzo in convenzione
- Responsabile delle Facilities: Soggetto terzo in convenzione
- Referente NIS: SC Analisi e Sviluppo Sistemi di Controllo

4. DOCUMENTI DI RIFERIMENTO

1. Politica per la Sicurezza delle Informazioni della ACSS
2. Linee Guida per gli Operatori di Servizi Essenziali – Autorità NIS-Settore Salute – luglio 2019
3. Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS)
4. Decreto del Direttore Della Repubblica 16 aprile 2013, n. 62: Regolamento recante codice di comportamento dei dipendenti pubblici
5. Decreto del Direttore del Consiglio dei ministri 6 novembre 2015, n. 5 recante “Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva”. Testo coordinato con le disposizioni contenute nel DPCM 2 ottobre 2017, n. 3
6. Linee guida regionali per l'adozione dei piani di organizzazione Aziendale delle aziende sanitarie e degli IRCCS di diritto pubblico della Regione Lombardia (DGR n. IX/3822 del 25.07.2012)
7. Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS)
8. D.lgs. 65/2018: Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione” (Attuazione Direttiva (UE) NIS 2016/1148) aggiornato dal Decreto-Legge 14 giugno 2021, n. 82
9. D.lgs. 38/2014: Attuazione della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, nonché della direttiva 2012/52/UE, comportante misure destinate ad agevolare il riconoscimento delle ricette mediche emesse in un altro stato membro

LINEA GUIDA CONTINUITÀ OPERATIVA

I sistemi informativi di ACSS sono parte essenziale ed indispensabile per lo svolgimento delle funzioni istituzionali ed è necessario quindi garantirne la sicurezza attraverso la salvaguardia della confidenzialità, dell'integrità e non ultimo della disponibilità.

La continuità delle risorse informative della ACSS è parte integrante dei processi e delle politiche di sicurezza dell'Agenzia e rappresenta quindi un impegno importante per garantire la continuità dell'attività di ACSS, sebbene l'Ente non eroghi servizi al cittadino e pertanto non detenga servizi critici.

1. INTRODUZIONE

ART 1) SCOPO

L'obiettivo della presente Linea Guida è quello di indirizzare, attraverso un modello strutturato, la progettazione e l'implementazione di un sistema di gestione della continuità operativa (di seguito sistema di BCM) dell'ACSS, in linea con quanto previsto dalle linee guida nazionali e dagli standard nazionali ed internazionali in materia di Business Continuity. La continuità operativa dell'ACSS dipende dalla piena disponibilità della connettività e del sistema informativo aziendale.

ART 2) CAMPO DI APPLICAZIONE

Il presente documento si applica a tutte le funzioni svolte dalla ACSS, per le quali si intende preservare la continuità operativa. Per quanto applicabile, tali indirizzamenti si intendono estesi anche ai servizi in Cloud.

La linea guida fornisce delle raccomandazioni che devono intendersi come riferimento per l'attuazione di quanto previsto in tema di continuità operativa dalla *Politica per la Sicurezza delle Informazioni* emanata dalla ACSS.

ART 3) DEFINIZIONI

Ai fini del presente documento, devono intendersi le seguenti definizioni.

Definizioni	Descrizione
Asset ICT	Si intendono le risorse informatiche dell'Organizzazione (es. PC, server, apparati di rete, apparati di sicurezza, software di base, software applicativo, software middleware, ecc.), a supporto dell'erogazione dei servizi critici della ACSS.
Azione Correttiva	È una un'azione definita e finalizzata ad eliminare la causa di una non conformità, e a prevenirne il nuovo accadimento.

Business Impact Analysis (BIA)	L'attività di valutazione degli impatti (conseguenze) sull'operatività di un'Organizzazione, derivanti dal verificarsi di un evento/disastro che ne causa la l'indisponibilità (parziale o totale).
Continuità Operativa ICT (CO)	La capacità di un'Organizzazione di adottare misure di reazione e contenimento ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'Organizzazione, il normale funzionamento delle e funzioni istituzionali. Ai sensi dell'art. 32 del GDPR, la continuità operativa è intesa come la capacità di un'Organizzazione di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Emergenza o crisi	È un evento ad elevato impatto negativo che può minacciare il perseguimento della mission istituzionale provocando ingenti danni.
Disaster recovery (DR)	L'insieme delle misure tecniche e organizzative adottate per assicurare all'Organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'Organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate.
Disastro	L'effetto di un evento improvviso che ha come impatto gravi e prolungati danni e/o perdite per l'Organizzazione.
Piano di Continuità Operativa o Piano di Business Continuity (PCO)	Documento operativo che descrive tutte le attività e le modalità finalizzate al ripristino della disponibilità delle risorse informative. Dal momento che la realtà ha dimensioni limitate e non sono erogati servizi/processi critici, soprattutto sotto il profilo ICT, il Piano di Continuità Operativa e il Piano di DR possono coincidere ma dovrà comunque essere presente la componente dedicata al Disaster Recovery.
Piano di Disaster Recovery (PDR)	Documento operativo che descrive tutte le attività necessarie a garantire, a fronte di un evento negativo di significativa rilevanza, che determini l'indisponibilità delle risorse informative a supporto dei servizi/processi critici individuati dall'Organizzazione, il ripristino degli stessi, entro un arco temporale predefinito, tale da minimizzare il più possibile le interruzioni nell'erogazione dei servizi. Si evidenzia che il PDR è la sezione del PCO che descrive le attività di ripristino del sistema informativo, costituisce parte integrante del PCO e stabilisce le misure tecniche ed organizzative per assicurare l'erogazione dei servizi classificati come critici (e delle procedure e applicazioni informatiche correlate) tramite le risorse HW, SW e di connettività presso un CED alternativo a quello/quelli di produzione.
Risorse Informative	I dati, le informazioni, le risorse informatiche, i supporti digitali e cartacei di archiviazione.
Risk Assessment (RA)	L'analisi per determinare il valore dei rischi di accadimento di un evento che possa interrompere l'erogazione di un servizio.
Risk Treatment (RT)	Trattamento del rischio a valle della sua individuazione (RA) al fine di contenerlo entro limiti accettabili per l'Organizzazione.
Recovery Point Objective (RPO)	Indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto.

Recovery Objective (RTO)	Indica il tempo di ripristino del servizio: è la durata di tempo entro il quale un processo critico ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili.
Stato di emergenza o di crisi	Situazione formalmente dichiarata di interruzione o deterioramento grave di uno o più processi critici o a rilevanza sistemica in seguito a disastri.
Studio di fattibilità tecnica (SFT)	Lo studio sulla base del quale l'Organizzazione deve adottare il PCO e il PDR.

Tabella 1 – Definizioni

ART 4) ACRONIMI

Ai fini del presente documento, sono adottati i seguenti acronimi.

Acronimo	Descrizione
BC	Business Continuity
BCM	Business Continuity Management
BIA	Business Impact Analysis
CED	Centro Elaborazione Dati
CO	Continuità Operativa
DR	Disaster Recovery
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
ICT	Information & Communication Technology
PCO	Piano di Continuità Operativa
PDR	Piano di Disaster Recovery/Disaster Recovery Plan
RA	Risk Assessment
RPO	Recovery Point Objective
RT	Risk Treatment
RTO	Recovery Time Objective
SFT	Studio di fattibilità tecnica

Tabella 2 – Acronimi

ART 5) CONTINUITÀ OPERATIVA

Come premesso, la continuità operativa di ACSS può essere compromessa in caso eventi/crisi che vanno a impattare sulla connettività e sui sistemi informativi aziendali. Di seguito si fornisce l'elenco degli applicativi a disposizione dell'ACSS.

Il presente documento si applica a tutte le funzioni svolte dalla ACSS, per le quali si intende preservare la continuità operativa. Per quanto applicabile, tali indirizzamenti si intendono estesi anche ai servizi in Cloud.

APPLICATIVO
Firma Digitale Documenti
PEC

Conservazione digitale
AMC (Cedolini, Fiscalità, Fatture, Pagamenti)
Protocollo, Delibere, Determine
Sito Internet/Intranet
Ecosistema Digital Monitor
Connettività e Sistemi di Videoconferenza
Sistema Rilevazione Presenze/Assenze
Piattaforma Microsoft 365

ART 6) IL MODELLO PER IL SISTEMA DI BCM

Affinché l'ACSS possa sviluppare una continuità aziendale adeguata al livello ed al tipo di impatto dell'Organizzazione, a seguito di un'interruzione della possibilità di svolgere le proprie attività, è opportuno adottare un sistema di BCM, che sia in linea con gli standard di riferimento, nonché con quanto previsto dalle normative applicabili. Tale sistema, si basa su un modello organizzato in cinque fasi, rappresentate nella figura seguente:



Figura 1 Modello del Sistema di BCM

Di seguito la descrizione sintetica delle suddette fasi:

- a. **Definizione:** prevede l'individuazione dell'ambito del sistema di BCM in termini di servizi/processi, strutture organizzative, terze parti interessate, politiche e risorse informative a supporto;
- b. **Assessment:** prevede l'analisi dei servizi/processi critici inclusi nell'ambito del sistema di BCM, l'analisi degli impatti sui servizi/processi critici inclusi nell'ambito del sistema di BCM derivante da situazioni di indisponibilità delle risorse informative a supporto e l'analisi del rischio per l'individuazione delle aree critiche e delle contromisure da adottare;
- c. **Pianificazione:** prevede la definizione della strategia di Business Continuity sulla base di quanto rilevato in fase di Assessment e la conseguente progettazione e la pianificazione della soluzione tecnica-organizzativa che assicuri la continuità operativa servizi/processi critici in relazione ai requisiti di RTO e RPO individuati nella fase precedente. La fase prevede inoltre la definizione del PCO e del PDR;
- d. **Attuazione:** prevede l'implementazione della soluzione tecnica-organizzativa individuata nella fase precedente nonché la comunicazione/sensibilizzazione e la formazione specifica del personale della ACSS e delle terze parti interessate sui piani di continuità operativa;
- e. **Revisione:** prevede il monitoraggio dell'efficacia/efficienza del sistema di BCM implementato, attraverso test e simulazioni dei piani, valutazioni delle performance, verifiche interne di conformità ed adeguatezza, mantenimento del PCO, del Piano di DR (di seguito anche PDR) e riesame della direzione. Tale fase prevede inoltre l'evoluzione del sistema in relazione ai feedback derivanti dalle suddette attività e da eventuali ulteriori requisiti interni ed esterni sopraggiunti nel frattempo.

Nei seguenti capitoli è descritto il dettaglio delle attività afferenti alle singole fasi del suddetto modello.

1.1.1 FASE 1: DEFINIZIONE



La fase di Definizione del sistema di BCM si articola nelle seguenti attività, descritte nei paragrafi successivi:

- Ambito del sistema di BCM;
- Politica per la Continuità Operativa;
- Organizzazione, ruoli e responsabilità del sistema BCM.

1.1.1.1 AMBITO DEL SISTEMA DI BCM

Il sistema di BCM è lo strumento con cui un'Organizzazione garantisce la capacità di continuare ad esercitare la propria missione istituzionale a fronte del verificarsi di eventi di gravità tale da compromettere la normale operatività, stabilendo le idonee misure preventive e correttive.

A tal fine, l'ambito del sistema di BCM definito dalla ACSS deve comprendere almeno:

- I processi correlati alle funzioni istituzionali dell'ACSS inclusi nel sistema di BCM, con l'obiettivo di rappresentare compiutamente il dominio di continuità, sebbene non vi siano servizi istituzionali "critici" per i quali deve essere garantita la continuità operativa;
- Le unità organizzative e le relative risorse umane della ACSS e le terze parti interessate (clienti, fornitori, ecc.), tenendo conto della sua ubicazione, dimensione, natura e complessità;
- Le risorse informative per cui si ambisce a mantenere la continuità operativa;
- Le componenti di connettività locale e/o remota/geografica a supporto;
- Le relazioni fra tutte le risorse indicate ai punti precedenti, al fine di rappresentare compiutamente l'ambito di continuità operativa;
- Le misure per garantire la continuità di funzionamento del sistema informativo a supporto dei servizi critici della ACSS.

1.1.1.2 POLITICA PER LA CONTINUITÀ OPERATIVA

È opportuno che la ACSS definisca una politica interna sulla continuità operativa da comunicare a tutto il personale e, laddove necessario, alle terze parti interessate, in modo che le iniziative intraprese in merito, siano congruenti con quanto in essa definito. Tale politica deve esplicitare la necessità di:

- Assicurare l'adozione ed il mantenimento di un processo per l'identificazione dei potenziali scenari di indisponibilità e degli impatti di tali scenari sui propri processi, al fine di definire un sistema in grado di migliorare la resilienza, la capacità di ripristino e di reazione a fronte di una crisi;
- Stabilire obiettivi e strategie per assicurare la continuità dell'attività;
- Individuare i ruoli previsti nel modello organizzativo per la gestione degli eventi di crisi;
- Definire un processo di comunicazione cui attenersi, al verificarsi di situazioni di crisi, con particolare riferimento sia alle comunicazioni interne che a quelle esterne (es. clienti finali, utenti finali, organi di informazione).

1.1.1.3 ORGANIZZAZIONE, RUOLI E RESPONSABILITÀ DEL SISTEMA DI BCM

In considerazione della realtà di dimensione limitata di ACSS e dell'assenza di servizi erogati al cittadino, la continuità operativa, nell'ambito della propria Organizzazione verrà gestita/garantita dal Responsabile della continuità operativa che in ACSS è individuato nel Responsabile IT e della Sicurezza delle informazioni. Tale figura è responsabile di supportare

la ACSS nella predisposizione di tutte le misure necessarie per ridurre l'impatto di un'emergenza e reagire prontamente ed efficacemente, in caso di un'indisponibilità delle risorse informative dovuta a un disastro.

Tale ruolo prevede, in *condizioni di emergenza* (crisi), le seguenti responsabilità:

- Assumere il controllo di tutte le operazioni e assumere le responsabilità sulle decisioni per affrontare l'emergenza, ridurre l'impatto e soprattutto ripristinare le condizioni preesistenti;
- Valutare le situazioni di emergenza e dichiarare dello stato di emergenza;
- Avviare le attività di ripristino delle risorse informative e controllare il loro svolgimento;
- Gestire i rapporti con l'esterno e delle comunicazioni ai dipendenti;
- Attivare il monitoraggio del processo di rientro dall'emergenza;
- Effettuare la dichiarazione di conclusione dello stato di emergenza (ritorno allo stato di normale operatività).

Ha la facoltà di avvalersi operativamente della collaborazione di:

- Personale tecnico specialistico appartenente alla ACSS;
- Consulenti esterni, ingaggiati mediante specifici contratti di servizio;
- Servizi di terza parte, erogati da società con competenze ed esperienze di continuità operativa e disaster recovery;
- Fornitori coinvolti nelle attività di CO/DR;

1.1.2 FASE 2: ASSESSMENT



In questa fase è opportuno che la ACSS conduca un'attività volta a valutare l'impatto di un evento critico sulle attività condotte ACSS attraverso le risorse informative, derivante dalla loro indisponibilità e le contromisure da adottare a seguito di una situazione avversa (es. indisponibilità temporanea o disastro), per contenere il rischio entro livelli accettabili.

A tale scopo, la fase di Assessment prevede un'analisi di impatto e una di rischio. Nel primo caso si ritiene essenziale valutare l'impatto di indisponibilità derivante dall'interruzione dei processi che supportano lo svolgimento delle attività ordinarie. Tale valutazione deve essere basata su due dimensioni di analisi:

- Categorie d'impatto, suddivise ad esempio in Perdita di Immagine, Perdite Finanziarie (minori ricavi), Violazione Normativa, Danni all'Incolumità delle Persone;
- Livelli di impatto, rappresentati a più livelli (es. Alto, Medio Alto, Medio, Medio Basso, Basso o Assente).

Le suddette valutazioni devono essere effettuate presumendo la totale assenza di contromisure o controlli di sicurezza eventualmente già implementati, al fine di garantire giudizi valutativi indipendenti dal contesto fisico, ambientale e tecnologico, che saranno trattati successivamente in sede di Risk Assessment.

Si ritiene di indicare le priorità di ripristino delle risorse informative; il tempo massimo di ripristino (RTO – Recovery Time Objective); il livello minimo delle risorse informative necessarie per recuperare la relativa disponibilità; i Clienti chiave, i fornitori e le altre terze parti coinvolte e i vincoli sotto cui operano il servizio e gli annessi processi (contrattuali, legali, regolati da normative interne o dalla legislazione vigente).

Uno dei risultati fondamentali della BIA, consiste nella definizione degli indici RTO (Recovery time Objective) e RPO (Recovery Point Objective), che rivestono particolare importanza in quanto consentono di individuare le tempistiche entro cui deve avvenire il ripristino desiderato.

In particolare:

- il Recovery Point Objective (RPO): rappresenta la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup o duplicazione) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto;
- il Recovery Time Objective (RTO): rappresenta la durata di tempo entro il quale un processo deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili per l'Organizzazione.

1.1.2.1 RISK ASSESSMENT e RISK TREATMENT

Per quanto riguarda l'analisi di rischio, svolta dal *Responsabile della Continuità Operativa* con il supporto delle parti interessate (interne o esterne alla ACSS) ha i seguenti obiettivi principali:

- Individuare gli scenari di indisponibilità (minacce) associati alle funzioni principali svolte dalla ACSS e valutare le rispettive probabilità di accadimento;
- Individuare le vulnerabilità degli asset ICT a supporto di tali funzioni e identificare il livello di rischio derivante dagli scenari di indisponibilità applicati (es. attacco informatico).

Una volta individuato il livello di rischio è necessario procedere al suo trattamento, per il quale risulta necessario valutare il giusto equilibrio tra i seguenti elementi:

- I risultati del Risk Assessment;
- Il rispetto delle norme cogenti;
- L'obiettivo di rischio massimo tollerabile su tutti gli asset coinvolti;
- Eventuali Piani di Rientro già approvati;
- Le necessità legate alla missione istituzionale;
- I costi necessari a sostenerla (es. tecnologiche, organizzazione).

Le possibili strategie di trattamento del rischio sono declinate nelle seguenti opzioni:

- *Evitare*: evitare il rischio, rinunciando, ad esempio, alle attività che lo generano;
- *Trasferire*: trasferire il rischio ad altre parti, come ad esempio assicuratori e fornitori;

- **Ridurre:** ridurre il rischio ad un livello accettabile predefinito dalla ACSS, attraverso l'implementazione delle opportune contromisure di sicurezza;
- **Accettare:** se non si ritiene opportuna alcuna delle precedenti opzioni.

Nell'ipotesi in cui si decida di ridurre o mitigare i rischi evidenziati ad un livello ritenuto accettabile, è necessario dotarsi di un sistema di contromisure tale da contrastare adeguatamente tali rischi, in termini di:

- Prevenzione delle minacce e degli attacchi al fine di ridurre il potenziale rischio di danni;
- Reazione agli attacchi, onde evitare, contenere o minimizzare i danni;
- Investigazione a supporto delle attività di analisi e valutazione dei danni subiti in seguito ad un attacco;
- Ripristino a supporto delle attività di ricostruzione della situazione antecedente il danno.

1.1.3 FASE 3: PIANIFICAZIONE



Le attività previste dalla fase di Pianificazione delle attività per la realizzazione del sistema di BCM, descritte nei paragrafi successivi, sono:

- La definizione della strategia di continuità operativa;
- L'analisi di fattibilità e la progettazione della soluzione tecnica/organizzativa;
- La definizione del PCO;
- La predisposizione del piano di attuazione del piano di CO.

1.1.3.1 DEFINIZIONE DELLA STRATEGIA DI CONTINUITÀ OPERATIVA

La definizione di una strategia di continuità operativa consente di indirizzare la soluzione tecnico-organizzativa per garantire la possibilità di proseguire le attività ordinarie della ACSS, riducendo al minimo gli impatti negativi, sulla base dell'analisi dei risultati della precedente fase di Assessment. In particolare, la strategia di continuità operativa, illustrata nella seguente figura, deve tenere conto dei seguenti fattori:

- Gli impatti sulle funzioni svolte dalla ACSS, derivanti da un'interruzione del servizio;
- I valori di RTO/RPO;
- I valori di rischio in rapporto a specifiche inadeguatezze dell'infrastruttura di sicurezza, piuttosto che di assenza di opportune misure di protezione e le contromisure individuate per il contenimento di tale rischio.

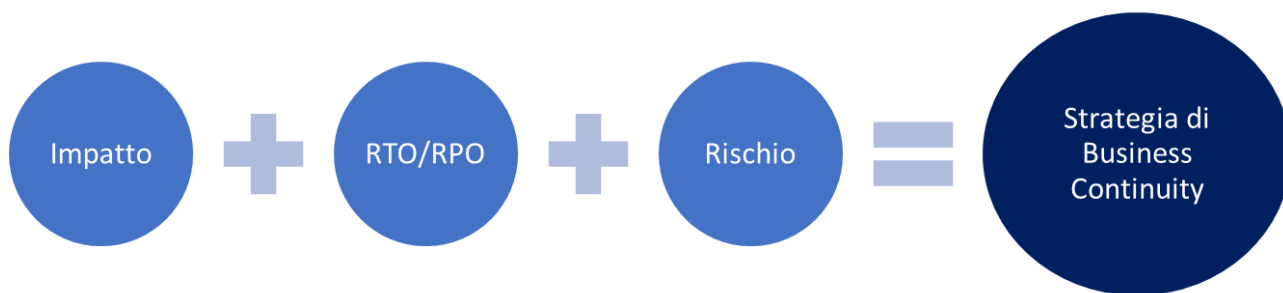


Figura 2 – Strategia di Continuità Operativa

1.1.3.2 ANALISI DI FATTIBILITÀ E PROGETTAZIONE SOLUZIONE TECNICA/ORGANIZZATIVA

Una volta definita la strategia di continuità operativa più opportuna, è necessario che il *Responsabile della Continuità Operativa*, con il supporto delle parti interessate (interne o esterne alla ACSS), effettui un'analisi di fattibilità tecnica per identificare gli interventi tecnico-organizzativi finalizzati a garantire la continuità operativa.

1.1.3.3 ANALISI DI FATTIBILITÀ TECNICA

L'analisi di fattibilità tecnica deve tener conto dei seguenti elementi minimali di valutazione/criticità:

- Analisi dei costi e vincoli di budget eventuali;
- Necessità di interventi di razionalizzazione preventiva (consolidamento, virtualizzazione, ecc.), in special modo prima di adottare soluzioni di DR;
- Esigenze logistiche, HW, SW, risorse umane;
- Necessità di competenze tecniche specifiche.

L'analisi di fattibilità tecnica è condotta o coordinata dal *Responsabile della Continuità Operativa* e deve contenere almeno le seguenti informazioni:

- Informazioni Generali: la descrizione della ACSS, dell'organizzazione interna, delle funzioni istituzionali;
- L'ambito dello studio/analisi di fattibilità: le attività ordinariamente svolte;
- Il risultato della fase di assessment;
- Le soluzioni tecnologiche e tecniche individuate: il dettaglio della soluzione o delle soluzioni che la ACSS ha individuato come rispondente/i alle proprie esigenze;
- Tempi e modalità implementative: in cui devono essere riportati, per tutte le soluzioni tecnologiche e tecniche individuate, i tempi e le modalità di realizzazione con l'indicazione di eventuali vincoli e rischi delle soluzioni.

1.1.3.4 PROGETTAZIONE SOLUZIONE TECNICA-ORGANIZZATIVA

A seguito dell'approvazione dello SFT da parte del *Comitato di Crisi*, deve essere effettuata, da parte del *Responsabile della Continuità Operativa* con il supporto delle parti interessate (interne o esterne

alla ACSS), la progettazione della soluzione tecnica-organizzativa, finalizzata alla predisposizione del PCO e del PDR.

La progettazione della soluzione è normalmente articolata nelle seguenti attività, formalizzate in documentazione specifica:

- Progettazione di alto livello del modello organizzativo/procedurale;
- Progettazione di alto livello della soluzione tecnologica;
- Progettazione di dettaglio del modello organizzativo/procedurale;
- Progettazione di dettaglio della soluzione tecnologica.

Il Piano di CO/DR deve di conseguenza prevedere, le modalità per reagire agli eventi nel modo più tempestivo possibile e stabilire un flusso di comunicazione ed attivazione efficiente ed efficace.

1.1.3.5 PIANO DI CONTINUITÀ OPERATIVA/DISASTER RECOVERY (PCO/PDR)

Il *Responsabile della Continuità Operativa* deve definire, con il supporto delle parti interessate (interne o esterne alla struttura) e sulla base dell'analisi di fattibilità svolta:

- Il PCO, che fissa gli obiettivi e i principi da perseguire nel rispetto dei tempi di RPO ed RTO individuati in fase di Assessment e descrive le procedure per la gestione della continuità operativa, anche qualora affidate a soggetti esterni. Il PCO tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive;
- Il PDR, che costituisce parte integrante di quello di continuità operativa di cui al punto precedente, stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti.

Il PCO è un documento complesso, normalmente articolato in più sezioni, che può contenere al suo interno documentazione di natura diversa come ad esempio procedure operative, organizzative, schede, elenchi di persone e di materiale, istruzioni operative.

Il PCO si compone di attività e fasi che devono essere dettagliatamente specificate e descritte: rappresenta pertanto una guida generale che indica come reagire ad eventi "negativi" di significativa rilevanza prima del ripristino entro determinati limiti di tempo.

Il PCO prevede l'esecuzione di chiare ed efficaci azioni, da parte dei soggetti coinvolti nel piano, come risposta alla situazione d'emergenza, all'eventuale stato di emergenza, e sono finalizzate al ripristino della situazione di normalità.

Nel PCO e in tutta la documentazione che lo compone, devono essere presenti le seguenti informazioni minimali:

- I ruoli e le responsabilità delle persone e dei gruppi di lavoro coinvolti;
- Il processo per l'attivazione dello stato di emergenza;
- Le informazioni per gestire le conseguenze immediate di una condizione di emergenza, tenendo in considerazione i seguenti fattori:
 - Le strategie, le tattiche e l'operatività per rispondere ad una condizione di emergenza;
 - La prevenzione di ulteriori perdite e/o indisponibilità;

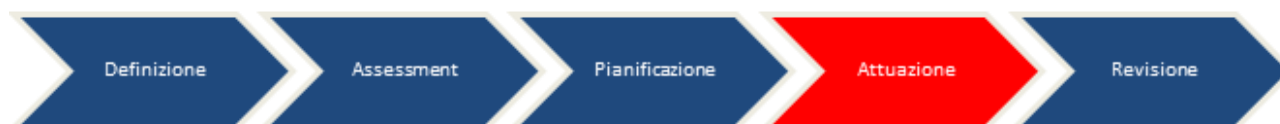
- Le informazioni su come ed in quali circostanze la ACSS effettuerà attività di comunicazione con i propri dipendenti;
- Le informazioni su come la ACSS continuerà le proprie attività o su come verranno ripristinate (in caso di DR) nell'ambito degli RTO e degli RPO definiti.

Il PCO e tutta la documentazione che lo compone devono essere definiti ed approvati dal *Comitato di Crisi*, specialmente la documentazione che conferisce opportuni poteri e responsabilità ai vari ruoli individuati durante la fase di emergenza.

1.1.3.6 PIANO DI ATTUAZIONE

Una volta effettuata la progettazione della soluzione tecnica-organizzativa, definito e approvato il PCO, occorre sviluppare il relativo piano di attuazione. Tale piano, coordinato dal *Responsabile della Continuità Operativa* e attuato con il supporto delle parti interessate (interne o esterne alla struttura), deve contemplare tutte le attività previste dal PCO ed essere in linea con i tempi implementativi descritti nell'analisi di fattibilità tecnica. Inoltre, per ogni attività riportata nel piano di attuazione, occorre individuarne la responsabilità implementativa.

1.1.4 FASE 4: ATTUAZIONE



Ai fini della realizzazione del piano di attuazione del sistema di BCM precedentemente definito, occorre effettuare le seguenti attività, descritte nei paragrafi successivi:

- Realizzare la soluzione tecnico/organizzativa individuata;
- Effettuare sessioni di comunicazione e formazione;
- Eseguire i test.

1.1.4.1 REALIZZAZIONE DELLA SOLUZIONE TECNICO/ORGANIZZATIVA DEFINITA

Nel realizzare la soluzione tecnica-organizzativa definita, nei modi e nei tempi previsti dal PCO/PDR e dal relativo piano di attuazione, la ACSS potrà ricorrere a fornitori esterni per dotarsi, attraverso forniture o servizi, di soluzioni di CO/DR.

1.1.4.2 COMUNICAZIONE E FORMAZIONE

Fase cruciale per la buona riuscita del PCO/PDR, è la formazione e sensibilizzazione del personale interno della ACSS e delle eventuali terze parti interessate, sul tema della continuità operativa e sul PCO, affinché ogni persona coinvolta, sia ben consapevole e addestrata sulle proprie attività da svolgere in caso di emergenza.

Tale attività, promossa e coordinata dal *Comitato di Crisi*, deve essere effettuata attraverso il coinvolgimento del *Responsabile della Continuità Operativa*, per la predisposizione di materiale

formativo, di checklist di verifica e soprattutto per l'organizzazione ed il coordinamento di sessioni di simulazione di casi reali.

1.1.4.3 TEST E RELATIVE MODALITÀ

Al termine della fase di realizzazione della soluzione tecnica-organizzativa, occorre verificarne l'efficacia e l'efficienza. A tal riguardo, il *Responsabile della Continuità Operativa* redige il piano di test, approvato dal *Comitato di Crisi*, che preveda una simulazione di emergenza quanto più esaustiva possibile.

1.1.5 FASE 5: REVISIONE



Un sistema di BCM deve essere sottoposto a regolare revisione, al fine di:

- Verificarne l'efficacia, l'efficienza e l'adeguatezza rispetto agli obiettivi prefissati ed alle politiche definite dalla ACSS;
- Identificarne le eventuali necessità di adeguamento, attuando le opportune azioni correttive e di miglioramento.

L'attività di revisione del sistema di BCM si concretizza attraverso:

- L'esecuzione di test ed esercitazioni simulate del PCO/PDR;
- La valutazione delle performance del sistema di BCM;
- Le Verifiche Interne del sistema di BCM;
- Il mantenimento del PCO/PDR;
- Il Riesame della Direzione;
- Il miglioramento del sistema di BCM.

Le suddette attività di revisione sono descritte nei paragrafi successivi.

1.1.5.1 TEST ED ESERCITAZIONI DI CO/DR

I test e le esercitazioni di continuità operativa devono essere eseguiti periodicamente (almeno una volta l'anno) dalle parti interessate (interne od esterne alla ACSS), e comunque ad ogni variazione dell'assetto tecnologico, tecnico, organizzativo, normativo, dei rapporti contrattuali e dei servizi critici erogati dalla ACSS. Il *Responsabile della Continuità Operativa* pianifica e coordina l'esecuzione di tali attività.

- Le attività di test riguardano prettamente il sistema informativo e la connettività, quindi l'aspetto tecnologico (test di Disaster Recovery).

La ACSS (o il fornitore, qualora venga richiesto un supporto esterno per svolgere i test), dovrà predisporre il test al fine di simulare una "vera" condizione di emergenza/indisponibilità prolungata

e, dovrà predisporre copie dei dati ad uso esclusivo della simulazione che saranno cancellate con modalità sicura, al termine dei test. L'avvenuta cancellazione di dette copie dei dati sarà verificata in contraddittorio dalle parti nei modi e tempi che saranno indicati.

Il piano relativo ai suddetti test ed i risultati derivanti dalla sua attuazione devono essere formalizzati per iscritto tramite, ad esempio, il verbale di test e il documento di tracciatura dell'esito delle prove effettuate. Il *Comitato di Crisi* deve approvare il piano di test esaminando altresì i risultati dei test eseguiti. Tale documentazione sarà analizzata nell'ambito delle fasi di Riesame della Direzione e di Miglioramento del sistema di BMC, al fine di indirizzare le opportune azioni correttive e/o di miglioramento.

1.1.5.2 VALUTAZIONE DELLE PERFORMANCE DEL SISTEMA DI BCM

La valutazione delle performance del sistema di BCM deve essere effettuata con periodicità almeno annuale da parte del *Responsabile della Continuità Operativa*. A tale scopo, è opportuno predisporre una procedura che descriva il processo monitoraggio, misurazione, analisi e valutazione delle performance del sistema di BCM. La procedura deve descrivere, come minimo:

- Cosa deve essere monitorato e misurato;
- I metodi da utilizzare per il monitoraggio, la misurazione, l'analisi e la valutazione;
- Le tempistiche per il monitoraggio e la misurazione;
- Le tempistiche per l'analisi e la valutazione dei risultati prodotti dal monitoraggio e dalla misurazione;
- Le metriche utilizzate per la definizione/misurazione dei Key Performance Indicator (KPI) individuati, in termini di modalità di calcolo, soglia attesa e frequenza di misurazione;
- Come i risultati delle suddette attività devono essere opportunamente documentati.

È opportuno che la ACSS conservi la documentazione che attesta i risultati emersi dalla valutazione delle performance del sistema di BCM, con evidenza delle eventuali non conformità rispetto ai risultati attesi. Tale documentazione sarà analizzata nell'ambito delle fasi di Riesame della Direzione (cfr. par. 7.5) e di Miglioramento del sistema di BMC (cfr. par. 7.6), al fine di indirizzare le opportune azioni correttive e/o di miglioramento.

1.1.5.3 VERIFICHE INTERNE

Con cadenza almeno annuale, il *Referente delle Verifiche Interne* della ACSS, deve predisporre il Piano annuale delle verifiche interne di continuità operativa, e provvedere alla loro esecuzione.

Tali verifiche sono finalizzate a verificare:

- La conformità del sistema di BCM ai requisiti di continuità formulati dalla ACSS e a quanto previsto dalla normativa vigente applicabile.

I risultati delle verifiche interne di continuità operativa devono essere documentati, evidenziando le eventuali non conformità riscontrate e/o le raccomandazioni di miglioramento emerse. Tale documentazione sarà analizzata nell'ambito delle fasi di Riesame della Direzione e di Miglioramento del sistema di BMC, al fine di indirizzare le opportune azioni correttive e/o di miglioramento.

1.1.5.4 MANTENIMENTO DEL PIANO DI CO/DR

Il PCO deve essere aggiornato ad ogni variazione significativa dell'assetto tecnologico, tecnico, organizzativo, normativo e dei rapporti contrattuali, da parte del *Responsabile della Continuità Operativa*, e deve essere vagliato ed approvato dal *Comitato di Crisi*, nel corso della riunione periodica indetta dal *Responsabile della Continuità Operativa* quando se ne rileva la necessità.

Anche il PDR, come sezione del PCO che descrive le attività di ripristino del sistema informativo, dovrà essere aggiornato ad ogni variazione significativa dell'assetto tecnologico, tecnico, organizzativo, normativo, dei rapporti contrattuali e dei servizi critici erogati dalla ACSS.

Si riportano di seguito, a titolo esemplificativo, alcune tipologie di eventi che devono essere presi in considerazione per l'aggiornamento del PCO/PDR:

- Modifiche dei fornitori e/o del contratto assicurativo;
- Modifiche dei servizi o delle applicazioni software (aggiunta/modifica/eliminazione di applicazioni, variazioni nella criticità delle applicazioni);
- Modifiche nell'hardware e/o nella rete;
- Stipula di nuovi contratti;
- Modifica delle normative applicabili.

Il verificarsi di uno o più di questi eventi, o comunque di un qualsiasi evento che possa incidere sull'efficacia del PCO/PDR, richiede quindi un'attenta analisi per valutare la necessità di apportare modifiche al Piano stesso.

1.1.5.5 RIESAME DELLA DIREZIONE

Il riesame della direzione ha l'obiettivo di assicurare nel tempo l'adeguatezza e l'efficacia del sistema di BCM attuato.

Gli elementi in ingresso al riesame della direzione comprendono:

- Lo stato di avanzamento delle azioni e delle raccomandazioni per il miglioramento previste dai precedenti riesami della direzione;
- I cambiamenti dei fattori interni ed esterni che hanno attinenza con il sistema di BCM, comprese le evoluzioni delle prescrizioni legali e delle altre prescrizioni relative ai propri aspetti ambientali;
- I risultati delle valutazioni sul rispetto delle prescrizioni legali e delle altre prescrizioni che l'organizzazione sottoscrive;
- I risultati delle attività di Revisione del sistema di BCM, comprensivi dei seguenti andamenti:
 - Risultati del monitoraggio e della misurazione delle performance;
 - Risultati delle verifiche interne;
 - Risultati dei test e delle esercitazioni periodiche.
- Il PCO/PDR;
- Le informazioni di ritorno e le comunicazioni provenienti dalle parti interessate esterne, compresi i reclami;
- I risultati delle attività di RA/RT;
- Ogni cambiamento, interno ed esterno, che può avere effetto sull'ambito del sistema di BCM;

- Le raccomandazioni per il miglioramento continuo;
- Tecniche, prodotti e procedure che possono essere utilizzate dalla ACSS per migliorare le prestazioni e l'efficacia del sistema di BCM;
- Eventuali standard e best practice emergenti;
- Lesson learned derivate da eventuali incidenti distruttivi.

Gli elementi in uscita al Riesame della Direzione devono comprendere decisioni relative alle opportunità per il miglioramento continuo ed ogni necessità di modifica al sistema di BCM, quali ad esempio:

- Modifiche all'ambito del sistema di BCM;
- Miglioramento dell'efficacia del sistema di BCM;
- Aggiornamento del RA, BIA, PCO/PDR e relative procedure;
- Modifiche a procedure e controlli per rispondere ad eventi interni o esterni alla ACSS, che possono aver impatto sul suo sistema di BCM, inclusi i seguenti cambiamenti:
 - Missione della ACSS;
 - Riduzione del rischio e requisiti di sicurezza;
 - Condizioni ambientali (es. evoluzione del contesto organizzativo, tecnologico) e processi;
 - Requisiti legali e normativi;
 - Obblighi contrattuali;
 - Livello di rischio e/o criteri per l'accettazione del rischio;
 - Necessità legate alle risorse;
 - Requisiti finanziari.
- Modifica dei criteri di misurazione dell'efficacia delle misure di continuità.

I risultati del riesame della direzione devono essere comunicati a tutte le parti (interne ed esterne) interessate. La ACSS deve inoltre conservare informazioni documentate quali evidenza dei risultati del riesame della direzione. Tale documentazione sarà analizzata nell'ambito della fase di Miglioramento del sistema di BMC, al fine di indirizzare le opportune azioni correttive e/o di miglioramento.

1.1.5.6 MIGLIORAMENTO CONTINUO

Nel corso dello svolgimento di attività legate principalmente ai Test ed alle esercitazioni di CO/DR, alla Valutazione delle performance, alle Verifiche Interne, al Riesame della Direzione, possono emergere delle non conformità o delle aree di miglioramento.

Nel caso in cui venga rilevata una non conformità, il *Responsabile della Continuità Operativa* deve coordinare ed indirizzare le parti interessate (interne od esterne alla ACSS), affinché eseguano le seguenti attività:

- Reazione alla non conformità e, per quanto applicabile, attuazione delle azioni di contenimento a fronte della non conformità e gestione delle conseguenze;
- Valutazione della necessità di azioni correttive per eliminare le cause della non conformità (root cause analysis), in modo che non si ripeta o non accada altrove. Le azioni correttive devono essere adeguate agli effetti delle non conformità riscontrate.

Nel caso invece, in cui venga evidenziata un'area di miglioramento, il *Responsabile della Continuità Operativa* deve coordinare ed indirizzare le parti interessate (interne od esterne alla ACSS) al fine di individuare le opportune azioni di miglioramento.

Le azioni correttive e di miglioramento individuate, devono essere sottoposte all'approvazione del *Comitato di Crisi*. A valle di tale approvazione, il *Responsabile della Continuità Operativa* deve, anche con il supporto le parti interessate (interne od esterne alla ACSS):

- Identificare, per ogni azione individuata, il responsabile dell'attuazione, i tempi e le risorse necessarie per la relativa implementazione;
- Attuare l'azione e verificarne l'efficacia;
- Attuare, se necessario, modifiche al sistema di BCM;
- Conservare la documentazione, quale evidenza della natura delle non conformità rilevate, delle aree di miglioramento, delle azioni correttive/di miglioramento intraprese e delle relative verifiche di efficacia effettuate.

2. DOCUMENTI DI RIFERIMENTO

1. Regolamento (UE) 679/2016 (GDPR);
2. D.lgs. 82/2005 – Codice dell'Amministrazione Digitale (CAD) e s.m.i
3. ISO/IEC 27001:2017 "Information technology — Security techniques — Information security management systems - Requirements", 2017-03
4. AgID "Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni", Agg.to 2013
5. AgID "Linee Guida razionalizzazione infrastruttura digitale della PA", 2013
6. ISO 22301:2019 "Societal security – Business continuity management systems – Requirements"
7. ISO 22313:2020 "Societal security – Business continuity management systems. Guidance"
8. ISO 22300:2018 "Societal security – Business continuity management systems. Terminology"
9. Information Technology Infrastructure Library (ITIL) v3
10. NIST SP 800-34 "Contingency Planning Guide for Federal Information Systems"
11. D.lgs. 65/2018: Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" (Attuazione Direttiva (UE) NIS 2016/1148)
12. Linee Guida per gli Operatori di Servizi Essenziali – Autorità NIS-Settore Salute – luglio 2019
13. Modello organizzativo Data Protection - ACSS
14. Politica per la Sicurezza delle Informazioni - ACSS
15. Ruoli e Responsabilità per la Sicurezza delle Informazioni - ACSS

POLITICA SPECIFICA PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA ICT

L'ACSS detiene, pertanto, un insieme organico e strutturato di misure di sicurezza logica, fisica, organizzativa e procedurale dedicate alla protezione dell'integrità, della riservatezza e della disponibilità delle informazioni e delle reti di comunicazione. La corretta gestione degli incidenti di sicurezza ICT è necessaria per evitare o minimizzare la compromissione dei dati contenuti all'interno del patrimonio informativo della ACSS in caso di incidente informatico ed inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti stessi.

In linea con tale approccio, la presente Politica declina un insieme di regole di base che indirizzano le strategie e le modalità di gestione degli incidenti di sicurezza informatica, stabilendo:

- Gli obiettivi di sicurezza;
- Le fasi del processo di gestione incidenti necessarie al raggiungimento degli obiettivi prefissati;
- I criteri e le metriche decisionali a supporto.

1. INTRODUZIONE

ART 1) SCOPO DEL DOCUMENTO

1. Gli orientamenti riportati nella presente Politica sono finalizzati a descrivere, in maniera chiara e comprensibile da tutto il personale della ACSS interessato, le attività relative al rilevamento, alla pre-analisi, alla classificazione ed al trattamento degli allarmi e degli incidenti di sicurezza ICT.

ART 2) CAMPO DI APPLICAZIONE

1. La presente Politica si applica a tutto il personale ed ai soggetti terzi della ACSS che vengono a conoscenza, in maniera diretta o indiretta, di un incidente di sicurezza occorso sui sistemi ICT posti sotto il dominio di competenza dell'Azienda.

ART 3) DEFINIZIONI E ACRONIMI

1. Ai fini dell'applicazione della presente Politica devono intendersi le seguenti definizioni:
 - **Agente malevolo:** Soggetto che, sfruttando le vulnerabilità insite in un sistema ICT ovvero sfruttando le proprie conoscenze derivanti dal ruolo organizzativo rivestito, causa, volontariamente o accidentalmente, una violazione delle politiche di sicurezza applicate ad un determinato asset ICT.

- **Autorità competente NIS:** Autorità settorialmente competente in materia di sicurezza delle reti e dei sistemi informativi (NIS). Il D.lgs. 65/2018 ha designato quali Autorità competenti NIS il Ministero della Salute per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza.
- **CSIRT Italia:** Il Computer Security Incident Response Team, di cui all'articolo 8 del decreto legislativo NIS.
- **Cybersecurity:** L'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza.
- **Dato Personale:** Dato personale ai sensi del GDPR: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Decreto legislativo NIS:** Il decreto legislativo 18 maggio 2018, n. 65.
- **Direttiva NIS:** Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, recepita in Italia con il decreto legislativo 18 maggio 2018, n.65.
- **Disponibilità:** Proprietà dell'informazione di essere accessibile e utilizzabile dal personale autorizzato, nei tempi, nei luoghi e nelle modalità adeguate alle necessità operative della ACSS.
- **Evidenza:** Qualsiasi elemento documentabile che contribuisce, con un adeguato margine di affidabilità, accuratezza ed esaustività, a definire le origini, le finalità, le modalità di svolgimento e gli eventuali danni attribuibili ad un determinato evento di sicurezza ICT.
- **Integrità:** Proprietà dell'informazione di essere presente, corretta e valida.
- **Minacce:** Insieme di eventi malevoli che possono agevolare una violazione delle politiche di sicurezza ICT ed un danno al patrimonio informativo della ACSS.
- **Patrimonio informativo:** Insieme di beni strumentali, materiali ed immateriali, che assumono un valore significativo per il compimento della missione della ACSS. Il patrimonio informativo è costituito dalle seguenti tipologie di risorse:

- Risorse tecnologiche: sistemi, apparati, infrastrutture hardware e software utilizzati come strumenti di supporto allo svolgimento dei processi della ACSS;
 - Informazioni: insieme composto da un'aggregazione di dati elementari, o da altre informazioni logicamente correlate tra di loro, funzionali allo svolgimento dei processi della ACSS;
 - Risorse umane: soggetti interni od esterni all'amministrazione che, attraverso il proprio patrimonio cognitivo e professionale, contribuiscono allo svolgimento dei processi della ACSS in un ambito di competenze e responsabilità predefinito;
 - Innovazioni, frutto dell'ingegno copyright e brevetti: qualsiasi elemento ascrivibile all'ambito di proprietà dell'amministrazione che costituisce fonte di vantaggio per lo svolgimento della missione di impresa e dei processi ad essa correlati.
- **Personale:** dipendente o assimilabile (es. contratti atipici).
 - **Riservatezza:** Caratteristica dell'informazione di essere conoscibile solo ad alcuni soggetti autorizzati.
 - **Soggetti terzi:** Fornitori, consulenti, collaboratori esterni, partner che operano con la ACSS in forza di un contratto.
 - **Strategia nazionale di sicurezza cibernetica:** La strategia di cui all'articolo 6 del decreto legislativo NIS.
 - **Violazione di sicurezza:** Azione o insieme di azioni intenzionali o accidentali, intraprese da un agente malevolo che comportano una elusione o inibizione delle politiche di sicurezza applicate ad un determinato asset ICT.
 - **Vulnerabilità:** Elemento caratteristico di un determinato asset ICT, che potrebbe essere sfruttato da agenti malevoli per apportare una violazione alle politiche di sicurezza ICT e/o per danneggiare il patrimonio informativo della ACSS.

2. Ai fini dell'applicazione della presente Politica devono intendersi i seguenti acronimi:

- **CSIRT:** Computer Security Incident Response Team.
- **GDPR:** General Data Protection Regulation.
- **DoS:** Denial of Service.
- **DDoS:** Distributed Denial of Service.
- **IDS:** Intrusion Detection System.
- **IPS:** Intrusion Prevention System.
- **NIS:** Network and Information Security.
- **OSE:** Operatore di Servizi Essenziali.
- **SIEM:** Security Information and Event Management.
- **SLA:** Service Level Agreement.

2. OBIETTIVI

ART 4) OBIETTIVI DI SICUREZZA PER LA GESTIONE INCIDENTI DI SICUREZZA ICT

1. Considerando la missione istituzionale ed il quadro normativo di riferimento, la ACSS si pone come obiettivo:
 - a. il rilevamento e la gestione tempestiva degli incidenti di natura informatica;
 - b. l'adozione di criteri decisionali oggettivi, verificabili e ripetibili, per la classificazione degli eventi di sicurezza e la definizione dei livelli di priorità nella gestione di tali eventi;
 - c. l'adozione di criteri decisionali per l'esecuzione delle *escalation* e il coinvolgimento di strutture esterne, quali CSIRT Italia, Garante per la protezione dei dati personali (di seguito anche "Garante Privacy"), Autorità competente per i Reati Informatici;
 - d. l'introduzione di attività continuative di miglioramento del grado di efficacia ed efficienza dell'intero processo di gestione incidenti.

3. GENERALITÀ

ART 5) PROCESSO DI GESTIONE DEGLI INCIDENTI ICT

1. Il processo di gestione degli incidenti di sicurezza ICT deve essere costituito da un insieme di attività ben definite, da compiersi in sequenza ordinata, secondo le seguenti macro-fasi:
 - **rilevazione degli eventi di sicurezza ICT:** attività finalizzata al monitoraggio, alla pre-analisi ed al tracciamento degli eventi di sicurezza ICT;
 - **classificazione degli eventi di sicurezza ICT:** attività finalizzata ad attribuire delle priorità di trattamento (secondo una metrica condivisa), e definire specifiche modalità per l'applicazione di misure di contenimento e/o contrasto agli eventi rilevati. A seconda della tipologia di classificazione dell'evento (allarme o incidente) si procede alla relativa modalità di gestione;
 - **gestione degli eventi di sicurezza ICT:** attività finalizzata a mitigare e contrastare le violazioni di sicurezza ICT riferite ad un determinato allarme o un determinato incidente di sicurezza, ivi comprese le attività di accertamento danni e ripristino alle condizioni standard antecedenti all'incidente stesso;
 - **analisi post-incidente di sicurezza ICT:** attività finalizzata all'analisi delle cause che hanno determinato l'incidente, con lo scopo di definire un piano di controlli migliorativi che permettono di contenere i rischi derivati da nuovi incidenti di simile natura;

- **miglioramento continuo:** attività finalizzata al miglioramento continuo dell'intero processo di gestione incidenti di sicurezza ICT.
2. Deve essere sviluppata una procedura operativa per la gestione degli incidenti di sicurezza ICT che recepisca formalmente gli indirizzamenti descritti nel presente documento, declinando al suo interno:
- a. ruoli e relative responsabilità coinvolte;
 - b. attività di dettaglio per ciascuna macrofase di cui all'Art. 5) comma 1;
 - c. livelli di servizio attesi (SLA).

ART 6) ORGANIZZAZIONE

1. Deve essere creato un gruppo di *incident handling* costituito da personale tecnico specialistico appartenente alla ACSS o da eventuali consulenti esterni con competenze ed esperienze specifiche nel monitoraggio, dedicato, secondo le modalità operative di seguito descritte, all'analisi e alla gestione degli eventi di sicurezza informatica.
2. All'interno del gruppo di *incident handling* possono essere individuati diversi livelli di responsabilità, con operatori di primo livello (responsabili del monitoraggio e rilevamento degli eventi) e una struttura di secondo livello per l'analisi e il coordinamento delle attività di gestione degli incidenti, secondo modalità di *escalation* delle responsabilità predefinite e concordate.

ART 7) TECNOLOGIE A SUPPORTO

1. L'ACSS è dotata di opportune piattaforme di sicurezza a supporto di tutte le attività di gestione incidenti, quali, a titolo esemplificativo e non esaustivo:
 - *sistemi Firewall*, posti a protezione delle reti controllate, cui è affidato il compito di rilevare, bloccare, tracciare e segnalare l'utilizzo di servizi/protocolli di rete e/o le richieste di accessi alla rete non conformi alle politiche di sicurezza implementate;
 - *sistemi IDS/IPS*, opportunamente dislocati nella rete interna, cui è affidato il compito di analizzare il traffico passante per rilevare, tracciare e segnalare eventi critici per la sicurezza ICT (tentativi di attacco via rete, scansioni di porte/servizi, tentativi di accesso, sfruttamento da remoto di vulnerabilità, ecc.);
 - *sistemi Antivirus*, cui è affidato il compito di rilevare, bloccare, tracciare e segnalare la propagazione di virus e altro software malevolo;
 - *sistemi Antispam*, cui è affidato il compito di rilevare, bloccare e segnalare la propagazione di posta elettronica indesiderata;
 - *sistemi Web Content Filtering*, cui è affidato il compito di limitare l'accesso ai siti Web non autorizzati;
 - *piattaforma SIEM*, cui è affidato il compito di raccogliere, centralizzare e correlare in tempo reale gli eventi rilevati generati dai sistemi sopra elencati.

Il sistema antivirus reso disponibile per ACSS da fornitore esterno è Ego Secure Data Protection.

2. Deve essere adottata un'opportuna soluzione tecnologica di supporto per la memorizzazione di tutti i dati relativi agli incidenti gestiti (*Knowledge Base* per le attività di gestione incidenti, accessibile esclusivamente dagli operatori del gruppo di *incident handling*). Tale sistema deve tracciare e archiviare tutte le informazioni prodotte durante le attività di gestione incidenti (descrizione degli eventi, sistemi interessati, azioni intraprese, riferimenti al personale coinvolto, comunicazioni intercorse, evidenze raccolte, ecc.), in modo da agevolare gli operatori nel riconoscimento di eventi già avvenuti e nella definizione del piano di contrasto e di ripristino.

4. RILEVAZIONE DEGLI EVENTI DI SICUREZZA ICT

ART 8) MONITORAGGIO DEGLI EVENTI DI SICUREZZA ICT

1. Il monitoraggio è l'insieme delle attività di controllo sistematico, finalizzate al rilevamento degli eventi ICT, ossia qualsiasi occorrenza che si verifica nell'ambito di un determinato asset informatico, la cui valenza è considerata significativa ai fini delle attività di gestione, controllo della sicurezza e contenimento dei rischi ad essa correlati. Tali attività sono svolte dagli operatori del gruppo di *incident handling*, ai quali sono assegnati i privilegi di accesso in lettura dei dati tracciati.
2. La segnalazione degli eventi di sicurezza ICT può provenire in diverse modalità, ossia:
 - **in modo automatico** dai sistemi informatici e dalle infrastrutture di sicurezza perimetrale (cfr. Art. 7) cui è affidato il compito di rilevare in tempo reale tutti gli eventi di sicurezza ICT occorsi nel dominio degli asset informatici e delle reti controllate;
 - **mediante estrazioni di log** prodotti dai dispositivi di monitoraggio o da altre piattaforme di sicurezza gestite (cfr. Art. 7) effettuate in autonomia dagli operatori del gruppo di *incident handling* per il rilevamento di *pattern* sospetti e/o eventi ripetuti, che possano evidenziare attività malevole;
 - **direttamente da parte di un utente** che utilizza i servizi informatici, o da un altro soggetto, che può rilevare eventi sospetti non rilevati dagli strumenti di monitoraggio sopra riportati e che presuppongano una violazione (o un tentativo di violazione) ai danni di uno o più sistemi posti sotto il dominio di responsabilità della ACSS, quali, ad esempio, alterazione di un sito web, un accesso non autorizzato a dati, indisponibilità di una risorsa ICT per un tempo prolungato, ecc. Le segnalazioni devono pervenire, in forma verbale o scritta, ad un punto di contatto della ACSS, che si occuperà di raccoglierle e valutarle.

ART 9) PRE-ANALISI DEGLI EVENTI DI SICUREZZA ICT

1. Gli eventi di sicurezza ICT segnalati dai sistemi di rilevamento automatizzato e tutte le comunicazioni provenienti da altre fonti (cfr. Art. 8), devono essere analizzati dagli operatori del gruppo di *incident handling* per individuare:
 - **gli asset ICT (sistemi/apparati) interessati dall'evento**, determinando con esattezza il contesto operativo dell'evento stesso, mediante la correlazione delle seguenti informazioni: *Evento* → *Indirizzo IP dei sistemi sorgente/destinazione* → *Sistema informatico coinvolto* → *Servizio coinvolto*;
 - **la categoria/sottocategoria dell'evento di sicurezza rilevato**, codificate a partire da una tassonomia standard e condivisa, in modo da garantire l'uniformità nella denominazione degli eventi facilitando le successive attività di classificazione, analisi e gestione. Ad esempio, è possibile far riferimento alla *Incident Classification Taxonomy* fornita da ENISA.
2. Gli operatori del gruppo di *incident handling* devono essere dotati, oltre che degli strumenti utilizzati in fase di rilevamento (cfr. Art. 8), di:
 - diagrammi di rete aggiornati (sia a livello logico, che a livello fisico), per reperire le informazioni relative ai componenti che compongono una rete e il modo in cui interagiscono (inclusi router, switch, firewall, etc.);
 - *asset inventory*, per poter estrarre le informazioni sulle catene tecnologiche dei servizi erogati e sulla relativa criticità dei sistemi informatici ad essi sottesi.
3. La procedura operativa di gestione incidenti di sicurezza ICT (cfr. Art. 5) deve contenere indicazioni circa gli SLA da rispettare per svolgere le attività di presa in carico e analisi degli eventi di sicurezza ICT.
4. Deve essere mantenuta ed aggiornata la lista degli **eventi precodificati (o Use Case)**, ossia gli eventi già analizzati, classificati e precedentemente trattati, per i quali le azioni di contrasto risultano preventivamente già definite e codificate in opportune istruzioni operative. Per questi tipi di eventi, gli operatori del gruppo di *incident handling* devono procedere in autonomia alle fasi di trattamento, attivando direttamente i sottoprocessi di gestione allarmi (cfr. Art. 16) o gestione incidente (cfr. Art. 17), secondo quanto definito nell'istruzione operativa specifica per l'evento precodificato, cui fa riferimento la segnalazione.
5. Le istruzioni operative per la gestione degli eventi precodificati devono contenere una descrizione dettagliata di tutte le operazioni di trattamento dell'evento di sicurezza ICT, ivi compresi i riferimenti operativi delle funzioni organizzative responsabili della gestione di sistemi/applicativi, da attivare e coordinare per la gestione degli eventi rilevati.

6. Le istruzioni operative per la gestione degli eventi precodificati devono essere mantenute aggiornate, recependo tutte le integrazioni derivanti da:
 - a. aggiornamenti tecnologici delle piattaforme di sicurezza utilizzate;
 - b. aggiornamenti nelle indicazioni in esse contenute, in particolare nel caso in cui queste non siano risultate completamente sufficienti al trattamento di specifici allarmi/incidenti.
7. Se a seguito delle analisi effettuate gli eventi si rivelassero dei **falsi positivi**, questi non genereranno degli allarmi, e pertanto gli operatori del gruppo di *incident handling* devono valutare la possibilità, tramite un *tuning* opportuno, di filtrare tali eventi dai sistemi di rilevamento per facilitare le attività di monitoraggio e analisi, evitando attività ripetitive.
8. Nel caso di **falso negativo**, ossia segnalazione proveniente direttamente da parte di un utente relativa ad un evento tecnologicamente rilevabile, ma non effettivamente rilevato dalle sonde di monitoraggio, gli operatori del gruppo di *incident handling* devono provvedere al *tuning* dei dispositivi di sicurezza necessario per garantire che i medesimi siano in futuro correttamente rilevati.
9. Nel caso di falso negativo riferito ad eventi non rilevabili dagli apparati di monitoraggio per specifici limiti tecnologici (ad esempio attacchi rilevati su canali non monitorati), gli operatori del gruppo di *incident handling*, prendono in carico l'evento e procedono con le successive attività di tracciamento (cfr. Art. 10), classificazione (cfr. Titolo V) e trattamento (cfr. Titolo VI).
10. Devono essere predisposte idonee procedure operative per l'esecuzione delle attività di *tuning* dei sistemi/apparati preposti al rilevamento e tracciamento degli eventi di sicurezza ICT.

ART 10) TRACCIAMENTO DEGLI EVENTI DI SICUREZZA ICT

1. Tutte le informazioni relative agli eventi di sicurezza ICT rilevati, le attività effettuate e le comunicazioni inviate ad eventuali gruppi, devono essere tracciate, nel rispetto della normativa vigente sulla protezione dei dati personali, su una apposita **scheda evento di sicurezza ICT**, che, nel corso del ciclo di vita dell'evento stesso, può essere riclassificata in scheda di gestione allarme o scheda di gestione incidente in base al cambiamento di stato dell'evento stesso.
2. L'archiviazione della scheda evento di sicurezza ICT deve essere effettuata su idonei supporti informatici, con caratteristiche tali da agevolarne in ogni momento la ricerca, la consultazione esclusivamente da parte del personale autorizzato e da garantirne l'integrità e la disponibilità (*Knowledge Base* per le attività di gestione incidenti, cfr. Art. 7). In questo

modo future occorrenze del medesimo evento (o di eventi comunque simili) potranno essere gestiti tempestivamente.

3. La scheda evento deve contenere le seguenti informazioni di dettaglio:
- a. identificativo univoco della scheda, utilizzabile per referenziare la scheda stessa;
 - b. tipo origine del rilevamento (automatizzato o non automatizzato);
 - c. data e ora del rilevamento dell'evento o della comunicazione ricevuta;
 - d. data e ora di apertura della scheda (qualora diverso dalla data di rilevamento dell'evento);
 - e. operatore che ha preso in carico l'evento;
 - f. identificativo mnemonico del sistema che ha effettuato il rilevamento dell'evento (es. IPS, FW, ecc.) o della provenienza della segnalazione (nel caso di rilevamento non automatizzato);
 - g. indirizzo IP del sistema/apparato dal quale si è originato l'evento (sorgente) e, quando disponibili, anche le seguenti informazioni: servizio, *hostname*, *mac-address*, sito, *owner*;
 - h. indirizzo IP del sistema/apparato target dell'evento (destinazione) e, quando disponibili, anche le seguenti informazioni: servizio, *hostname*, *mac-address*, sito, referente servizio e referente sistemi coinvolti;
 - i. categoria dell'attacco rilevato;
 - j. nel caso di rilevamento automatico da un dispositivo di sicurezza, le firme segnalate dal sistema di monitoraggio;
 - k. eventuali altri sistemi target interessati dall'evento ovvero potenzialmente a rischio a seguito dell'evento (in particolare gli altri elementi della catena tecnologica appartenente al servizio impattato);
 - l. eventuali altre indicazione o evidenze che hanno indotto gli operatori del gruppo di *incident handling* all'attribuzione della specifica classe (es. log di sistema, log applicativi o allarmi generati da altri sistemi/apparati);
 - m. stato di lavorazione della scheda.

5. CLASSIFICAZIONE DEGLI EVENTI DI SICUREZZA ICT

ART 11) GENERALITÀ

1. Gli eventi di sicurezza ICT analizzati, se non identificati come falso positivo, devono essere classificati, per poter formulare specifiche modalità operative di attuazione delle misure di contrasto/contenimento, commisurate all'effettivo grado di pericolosità dell'evento o dell'insieme di eventi rilevati ed al contesto operativo cui tali eventi si riferiscono.

2. Per conciliare la rapidità di intervento con l'affidabilità e l'accuratezza delle informazioni utili a definire le attività di trattamento, nella procedura operativa di gestione incidenti ICT (cfr. Art. 5) devono essere definiti gli SLA che stabiliscano il tempo massimo entro il quale devono essere effettuate le operazioni di classificazione e l'avvio delle attività di contrasto/contenimento degli allarmi/incidenti di sicurezza ICT.
3. La classificazione degli eventi da parte degli operatori del gruppo di *incident handling* deve procedere secondo le seguenti fasi:
 - valutazione della **criticità associata all'evento** rilevato;
 - valutazione della **tipologia dell'evento** rilevato;
 - definizione dei **livelli di priorità**;
 - avvio delle **attività di trattamento**.

6. CRITICITÀ DELL'EVENTO

ART 12) VALUTAZIONE DELLA CRITICITÀ DELL'EVENTO DI SICUREZZA ICT

1. La criticità dell'evento rilevato, che esprime la sua gravità all'interno del contesto di osservazione, deve essere calcolata dagli operatori del gruppo di *incident handling* in funzione:
 - a. del **potenziale di minaccia**, inteso come la pericolosità della minaccia (e degli attacchi ad essa associati), indipendentemente dal contesto in cui questa viene rilevata. Tale valore è fornito dai dispositivi automatici di rilevamento (generalmente indicato come *Severity*) espresso su di una scala ordinale a tre valori (Alto, Medio, Basso). Alternativamente può essere valutato in base alla competenza ed all'esperienza degli operatori del gruppo di *incident handling*, utilizzando la seguente metrica valutativa:
 - ALTO: Attacchi che comportano il rischio di una inaccettabile perdita di integrità, l'aggiramento dei meccanismi di non-ripudio, oppure che consentono ad un attaccante di livello medio il superamento di meccanismi di controllo, l'accesso immediato al sistema, l'accesso come super-utente, la non individuabilità/perseguibilità;
 - MEDIO: Attacchi che comportano una inaccettabile perdita di riservatezza e/o una grave perdita di disponibilità, oppure che forniscono ad un attaccante di livello medio informazioni atte ad effettuare escalation di privilegi e ad ottenere quindi con elevata probabilità l'accesso a parti critiche del sistema;
 - BASSO: Attacchi che comportano una interruzione parziale del servizio, oppure che forniscono informazioni potenzialmente pericolose, che se sfruttate possono portare ad una parziale compromissione del sistema o all'utilizzo inappropriato delle risorse informatiche.

b. del **grado di sensibilità dell'asset ICT** cui si riferisce l'evento o la combinazione degli eventi rilevati, espresso su di una scala ordinale a tre valori (Alta, Media, Bassa). Tale valore deve essere derivato dalla classificazione del servizio erogato così come riportata nell'*asset inventory* (cfr. Art. 9) o in una equivalente classificazione utilizzata all'interno del dominio di competenza della ACSS oppure determinato mediante idonee attività di *Risk Assessment* effettuate sugli asset ICT.

c. del **grado di vulnerabilità presunta degli asset ICT**, espresso su di una scala ordinale a tre valori (Alta, Media, Bassa). Tale valore rappresenta un giudizio sulla vulnerabilità intrinseca del target rispetto all'evento considerato e può essere dedotto:

- dalle configurazioni dei sistemi ICT, quali tipo e versione di sistema operativo, *patch level*, effettiva presenza sul sistema coinvolto delle vulnerabilità sfruttabili dalla minaccia che sottende l'attacco in corso, ecc.;
- dai risultati di una precedente attività di scansione (*Vulnerability Assessment*) effettuata sull'asset ICT.

2. La criticità dell'evento, funzione del *potenziale di minaccia dell'evento*, della *sensibilità dell'asset ICT* e della *vulnerabilità dell'asset ICT*, deve essere espressa su una scala di tre valori (Alta, Media, Bassa) secondo i criteri di attribuzione riportati nel seguente schema:

	Criticità dell'evento		
	Bassa	Media	Alta
Potenziale di Minaccia	Basso	Medio Alto	Basso Medio Alto
Sensibilità dell'Asset	Basso Medio	Basso Medio	Alto <u>Valore non Noto</u>
Vulnerabilità dell'Asset	Basso Medio	Basso Medio	Alto <u>Valore non Noto</u>

Tabella 1 - Metrica per l'assegnazione della criticità dell'evento

3. Facendo riferimento alla Tabella 1, la criticità dell'evento è definita dal verificarsi contemporaneo delle tre condizioni su potenziale di minaccia, sensibilità dell'asset e vulnerabilità dell'asset.

7. TIPOLOGIA DELL'EVENTO

ART 13) VALUTAZIONE DELLA TIPOLOGIA DELL'EVENTO DI SICUREZZA ICT

1. La tipologia dell'evento di sicurezza ICT, in aggiunta alla criticità dell'evento precedentemente definita (cfr. Art. 12), consente agli operatori del gruppo di *incident handling* di conseguire un ulteriore livello di dettaglio nella definizione dell'evento stesso,

utile ad indirizzare le successive attività di trattamento. Esso è determinato utilizzando la seguente metrica:

- a. **eventi di tipo Information:** eventi associati ad attività che non costituiscono di per sé un pericolo diretto al patrimonio informativo, ovvero a comportamenti anomali da parte di utenti e applicazioni che non necessitano di un particolare intervento di contenimento, se non di un'azione di monitoraggio per prevenire o contenere eventuali attacchi susseguenti. Ad esempio:
 - azioni di *enumeration* (ad es. allarmi tipo *ping sweep*) dei nodi attivi su una sottorete;
 - scansioni di porte TCP/UDP aperte (*port scan*) effettuato una sola volta o comunque su destinazioni non particolarmente sensibili;
 - accessi errati da parte di utenti che, pur comportando il blocco di una singola utenza, non denotano una particolare attività illecita mirata al DoS, o all'accesso non autorizzato;
 - allarmi determinati dalla presenza di software non autorizzato sui sistemi client.
- b. **eventi di tipo Warning:** eventi associati al rilevamento di un tentativo di violazione della sicurezza ICT per la quale devono essere attivate tutte le procedure di pronto intervento per la gestione dell'allarme. Ad esempio:
 - attività utente sospetta (accessi inusuali, tentativi di accesso multipli su sistemi differenti, tentativi di *privilege escalation* o di accesso ripetutamente falliti, che possano denotare attacchi di tipo *brute force*);
 - azione di *enumeration* sistematica e persistente che qualifichi realmente una fase di pre-attacco;
 - tentativi di attacchi DoS o DDoS che non hanno provocato il *crash* di un server o di un'intera rete;
 - codici malevoli che non creano un disservizio o un danno diretto al sistema target, riconosciuti e bloccati dal software antivirus;
 - segnalazioni di siti web o di *mail* di *phishing*.
- c. **eventi di tipo Critical:** eventi generati nel momento in cui viene effettuata una constatazione di possibile danno, permanente o temporaneo, al patrimonio informativo della ACSS. In particolare, tale tipologia costituisce la soglia di differenziazione tra allarmi ed incidenti, dove la discriminante per quest'ultimi è la presenza di danni reali, diretti o indiretti, agli asset ICT coinvolti. Ad esempio:
 - attacchi DoS o DDoS che provocano il *crash* di un server o di un'intera rete;
 - propagazione incontrollata di software malevolo auto replicante, non bloccato dai software antivirus, che infetta diversi sistemi di una medesima rete;
 - evidenze di accessi non autorizzati (ad es. tramite attacchi tipo SQL *Injection*);
 - evidenze di furto di credenziali utente, tramite attacchi applicativi (es. XSS) o tecniche di *password guessing*;
 - evidenze di compromissione di utenze amministrative.

8. PRIORITÀ DELL'EVENTO

ART 14) DEFINIZIONE DEI LIVELLI DI PRIORITÀ

1. Sulla base della criticità e della *tipologia dell'evento* deve essere definito il *livello di priorità di trattamento* che stabilisce i criteri decisionali per l'attribuzione delle urgenze per le specifiche attività di contrasto/contenimento, in particolare nell'evenienza in cui si debbano gestire più eventi di sicurezza ICT contemporanei.

La **priorità di trattamento**, secondo una scala ordinale a quattro valori (Bassa, Media, Alta, Massima), deve essere attribuita secondo la metrica illustrata nella tabella successiva:

Criticità dell'evento	Tipologia dell'evento	Priorità di trattamento
Bassa/Media	Information	Bassa
Bassa/Media	Warning	Media
Alta	Information	Media
Alta	Warning	Alta
Alta	Critical	Massima

Tabella 2 - Metrica per l'assegnazione della priorità di trattamento degli eventi di sicurezza ICT

2. Gli SLA presenti nella procedura operativa di gestione incidenti di sicurezza ICT (cfr. Art. 5), da rispettare per l'avvio delle attività di contrasto/contenimento, devono tenere in considerazione i livelli di priorità attribuiti agli eventi di sicurezza.

9. AVVIO ATTIVITÀ DI TRATTAMENTO

ART 15) AGGIORNAMENTO DELLA SCHEDA EVENTO

1. Le attività di valutazione della criticità e della tipologia degli eventi di sicurezza ICT di cui agli Art. 12) e Art. 13) svolte dagli operatori del gruppo di *incident handling* sono funzionali alla generazione di un:
 - a. **allarme di sicurezza ICT** (in caso di evento con tipologia "Information" o "Warning"): segnalazione, derivante dal rilevamento di uno o più eventi che non sottintendono una constatazione di danni per gli asset ICT ovvero per il patrimonio informativo della ACSS, per i quali sono comunque necessarie specifiche attività di monitoraggio e contenimento. Gli allarmi di sicurezza ICT si possono pertanto assimilare a tentativi di attacco o a prodromi di un attacco successivo;
 - b. **incidente di sicurezza ICT** (in caso di evento con tipologia "Critical"): qualsiasi evento o insieme di eventi che sottintendono una violazione delle politiche di sicurezza ICT fonte di danno per gli asset ICT ovvero per il patrimonio informativo della ACSS per i quali devono essere intraprese specifiche attività di contrasto nonché di ripristino delle condizioni standard antecedenti all'incidente.

1. Sulla base delle informazioni ricavate in fase di analisi e classificazione dell'evento, gli operatori del gruppo di *incident handling* devono provvedere ad aggiornare lo stato della scheda evento compilata originariamente (cfr. Art. 10) in **scheda di gestione allarme** o **scheda di gestione incidente** a seconda se gli eventi rilevati sono stati identificati rispettivamente come allarme o incidente di sicurezza ICT.
2. L'apertura di una scheda di gestione allarme attiva le attività di contrasto o contenimento degli allarmi segnalati (cfr. Art. 16) mentre l'apertura di una scheda di gestione incidente attiva il trattamento degli incidenti (cfr. Art. 17).

10.GESTIONE DEGLI EVENTI DI SICUREZZA ICT

ART 16) TRATTAMENTO DEGLI ALLARMI DI SICUREZZA ICT

1. Devono essere individuati e attuati tutti gli interventi finalizzati a contrastare e contenere le violazioni di sicurezza ICT cui sottintende un determinato allarme.
2. Qualora durante le attività di trattamento gli operatori del gruppo di *incident handling* individuino la necessità di effettuare degli interventi sui sistemi target interessati dall'allarme rilevato (ad esempio, rimozione sui sistemi di servizi di rete non utilizzati, blocco utenze, applicazione di security patch sui sistemi, ecc.), devono attivare le specifiche Unità Organizzative di competenza, inviando una richiesta con tutti i dettagli operativi necessari all'esecuzione dell'attività.
3. Al termine delle attività di trattamento, gli operatori del gruppo di *incident handling* devono disporre la chiusura formale della scheda allarme, annotandone la data e l'ora di chiusura, il personale coinvolto, le attività effettuate, i risultati ottenuti ed eventuali altre indicazioni/comunicazioni intercorse con le diverse strutture coinvolte. L'archiviazione di tali schede viene effettuata conformemente a quanto previsto all'Art. 10).
4. Qualora, nel corso delle attività di trattamento dell'allarme, vengano rilevati dei danni (diretti o indiretti) agli asset ICT come conseguenza di una violazione della sicurezza ICT, gli operatori del gruppo di *incident handling* devono provvedere ad aggiornare la scheda allarme, riclassificandola come incidente e riportando tutte le informazioni relative all'origine dell'incidente di sicurezza, procedendo con le attività di trattamento degli incidenti di sicurezza ICT descritte nell'Art. 17).

ART 17) TRATTAMENTO DEGLI INCIDENTI DI SICUREZZA ICT

1. Devono essere individuati e attuati tutti gli interventi finalizzati a contrastare e contenere le violazioni di sicurezza ICT cui sottintende un determinato incidente.
2. Una volta applicate le misure di contrasto/contenimento per bloccare l'incidente in corso, devono essere effettuate tutte le operazioni utili ad accertare, mediante la raccolta e l'analisi di evidenze, l'entità e la natura degli eventuali danni subiti interfacciandosi con il Responsabile del servizio impattato, le diverse Unità Organizzative interessate dall'incidente o altri specialisti esterni se necessario.
3. Sulla base dell'accertamento dei danni subiti e della loro valutazione, devono essere determinati gli elementi circostanziali che possono indurre una *escalation* dell'incidente verso altre Strutture esterne specifiche, quali:

a. **Garante Privacy**, in caso di violazioni di sicurezza (*data breach*) che comportano - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati tramite i sistemi informatici della ACSS.

In questi casi, il Titolare del Trattamento, senza ingiustificato ritardo, entro **72 ore** dalla constatazione dell'incidente, deve notificare la violazione al Garante, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. La notifica deve avvenire secondo le modalità indicate dal Garante stesso pubblicate sul relativo sito web (<https://servizi.gpdp.it/databreach/s/>). Inoltre, nel caso in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali degli Interessati, il Titolare deve darne comunicazione anche a ciascun Interessato al fine di consentirgli di adottare idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi dati personali, a meno che abbia già preso misure tali da ridurre l'impatto. La comunicazione all'Interessato deve essere effettuata utilizzando un linguaggio semplice e chiaro ed i canali più idonei.

b. **Autorità Competente per i Reati Informatici**, in caso di reati informatici perpetrati per mezzo o nei confronti dei sistemi informatici della ACSS, ossia quando l'incidente appartiene alle macrocategorie riportate di seguito secondo quanto indicato nel Codice penale:

- *frode informatica* (art. 640 ter del Codice penale);
- *accesso abusivo a un sistema informatico o telematico* (art. 615 ter del Codice penale);
- *detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici* (art. 615 quater del Codice penale);

- *diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico* (art. 615 quinquies del Codice penale);
- *intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* (artt. 617 quater e 617 quinquies del Codice penale);
- *falsificazione, alterazione, soppressione di comunicazioni e danneggiamento di sistemi informatici o telematici* (art. 617 sexies, 635 bis, ter, quater e quinquies, art. 420 del Codice penale).

La denuncia deve essere effettuata secondo le modalità indicate sul portale della Polizia di Stato (Polizia Postale: Homepage (commissariatodips.it)).

4. Dopo l'accertamento dei danni, deve essere redatto un rapporto di constatazione incidente di sicurezza ICT, da allegare alla scheda di gestione incidente, che deve evidenziare le seguenti informazioni:
 - a. data e ora di stesura del rapporto;
 - b. elenco delle verifiche svolte per rilevare e circoscrivere il perimetro entro il quale è stata rilevata la violazione della sicurezza ICT;
 - c. elenco degli eventuali danni subiti;
 - d. riferimenti alle evidenze comprovanti la constatazione dei danni subiti, senza allegare le evidenze stesse;
 - e. elenco dettagliato degli asset ICT che hanno subito i danni (sistemi, apparati, catene tecnologiche, applicazioni ecc.).
5. Deve essere definito il piano operativo degli interventi necessari per l'attuazione delle attività di ripristino (nei casi applicabili) alle condizioni standard antecedenti all'incidente.
6. Nel piano di ripristino devono essere riportate perlomeno le seguenti informazioni:
 - a. la descrizione dettagliata degli interventi programmati;
 - b. gli asset ICT interessati dagli interventi;
 - c. il gantt delle attività programmate;
 - d. le Unità Organizzative responsabili dell'implementazione/attuazione degli interventi di ripristino.
7. Il piano di ripristino deve essere allegato alla scheda incidente e sottoposto alle Unità Organizzative coinvolte che, ciascuna per il proprio ambito di competenze, sono responsabili:
 - a. della conduzione delle attività di ripristino alle condizioni standard antecedenti all'incidente, nei tempi e nei modi stabiliti dai rispettivi piani di ripristino;
 - b. della rendicontazione dello stato di avanzamento lavori osservando una periodicità definita opportunamente.

8. Al termine degli interventi di ripristino attuati, ciascun referente delle parti coinvolte nella gestione dell'incidente comunica la fine delle attività agli operatori del gruppo di *incident handling* che provvedono ad aggiornare e chiudere la scheda gestione incidente. L'archiviazione di tali schede viene effettuata conformemente a quanto previsto all'Art. 10).
9. Nel caso di incidente di sicurezza ICT con impatto *rilevante* sulla continuità dei servizi essenziali, precedentemente notificato secondo quanto definito al comma 3, lettera c), la ACSS deve effettuare una comunicazione al CSIRT italiano e all'Autorità Regionale NIS Competente circa la sua chiusura.
Nella suddetta comunicazione deve essere allegata un'apposita relazione sintetica che deve riportare le seguenti informazioni:
 - a. servizi e asset impattati;
 - b. durata e impatto dell'incidente;
 - c. le cause dell'incidente;
 - d. le attività svolte;
 - e. le misure di mitigazione adottate;
 - f. lo stato attuale delle reti e dei sistemi informativi.

Entro 20 giorni dalla comunicazione di fine incidente *rilevante* la ACSS invia al CSIRT italiano e all'Autorità Regionale NIS Competente un'apposita relazione di aggiornamento recante:

- a. la quantificazione dell'impatto sull'erogazione dei servizi essenziali;
- b. eventuali ulteriori elementi rilevanti.

11. ANALISI POST-INCIDENTE DI SICUREZZA ICT

ART 18) ANALISI POST-INCIDENTE DI SICUREZZA ICT

1. Alla conclusione delle attività di ripristino dell'incidente di sicurezza ICT, deve essere svolta, osservando tempistiche da definire opportunamente, l'analisi post-incidente. Tale processo consiste in una serie di attività programmate, volte a verificare:
 - a. le caratteristiche della minaccia responsabile dell'incidente;
 - b. le cause e le modalità di sviluppo dell'incidente, le circostanze e/o le vulnerabilità che lo hanno reso possibile;
 - c. un eventuale piano propositivo per il miglioramento dello stato della sicurezza che tenda a contenere i rischi di nuovi incidenti di simile natura.
2. L'analisi post-incidente deve comprendere le seguenti attività:
 - a. la raccolta dei dati relativi all'incidente;
 - b. l'analisi degli asset coinvolti;
 - c. l'analisi degli eventi correlati all'incidente;
 - d. la costruzione dello scenario causa-effetto;

- e. la valutazione degli impatti e potenziali propagazioni degli incidenti;
- f. la conservazione delle fonti di prova per fini probatori.

12.MIGLIORAMENTO CONTINUO

ART 19) MIGLIORAMENTO CONTINUO DEL PROCESSO DI GESTIONE INCIDENTI

1. Il processo di gestione incidenti di sicurezza ICT deve essere sottoposto ad una attività di controllo periodica, con cadenza almeno annuale, per consentirne il miglioramento e, conseguentemente, l'accrescimento del relativo livello di maturità. Devono essere pertanto effettuate le seguenti attività:
 - a. verifica dell'allineamento del processo di gestione incidenti con i requisiti strategici di gestione incidenti definiti dalla ACSS e con la normativa vigente;
 - b. analisi dei carichi di lavoro del personale coinvolto per verificare il corretto dimensionamento dello staff dedicato al processo di gestione incidenti;
 - c. valutazione efficienza/efficacia dell'attività di formazione tecnica rivolta agli operatori del gruppo di *incident handling*;
 - d. valutazione efficienza/efficacia dell'attività di *awareness* sul processo di gestione incidenti definito;
 - e. miglioramento continuo del processo a seguito delle attività di analisi post-incidente con il possibile coinvolgimento di altre Unità Organizzative e fonti esterne (evidenziando necessità di interventi tecnici, di ottimizzazione dei processi in vigore, di formazione/dimensionamento degli operatori di sicurezza ICT).
2. Per favorire il governo del processo di gestione incidenti di sicurezza ICT, deve essere avviato un processo di rendicontazione periodica, con cadenza da definire opportunamente, tramite la produzione di report contenenti specifici indicatori e dati riassuntivi sugli eventi, gli allarmi, gli incidenti e i falsi positivi gestiti nel periodo di riferimento distribuiti per servizio impattato e per le diverse piattaforme di monitoraggio utilizzate.

13.DOCUMENTI DI RIFERIMENTO

1. Regolamento UE n. 679/2016 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE – General Data Protection Regulation (GDPR)
2. D.lgs. 101/2018: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016,

- relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
3. Provvedimento del Garante Privacy del 30 Luglio 2019 sulla notifica delle violazioni dei dati personali (data breach)
 4. Legge 23 dicembre 1993 n. 547: Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica
 5. Legge 18 marzo 2008, n. 48: Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno
 6. Codice penale italiano
 7. Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS)
 8. D.lgs. 65/2018: Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" (Attuazione Direttiva (UE) NIS 2016/1148) Linee Guida per gli Operatori di Servizi Essenziali – Autorità NIS-Settore Salute – luglio 2019 allegate all'accordo n. 183/CSR del 7/11/2019 tra il Governo, le Regioni e Province autonome di Trento e Bolzano
 9. D.lgs. 38/2014: Attuazione della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, nonché della direttiva 2012/52/UE, comportante misure destinate ad agevolare il riconoscimento delle ricette mediche emesse in un altro stato membro
 10. Framework Nazionale per la Cybersecurity e la Data Protection
 11. ISO/IEC 27035:2011, "Information technology - Security techniques – Information security incident management"
 12. NIST Special Publication 800-61, "Computer Security Incident Handling Guide"
 13. ENISA - "Reference Incident Classification Taxonomy. Task Force Status and Way Forward"

POLITICA SPECIFICA PER GLI AMMINISTRATORI DI SISTEMA

Gli Amministratori di Sistema sono una categoria di operatori preposti all'esercizio dei sistemi informatici che, in funzione dei compiti ad essi assegnati, occupano i vertici della gerarchia delle utenze, in termini di privilegi di accesso alle risorse informatiche e ai dati ivi custoditi. Per tali motivi, il processo di attribuzione degli incarichi di Amministratore, così come la definizione dei relativi profili e permessi di accesso, riveste un carattere di estrema importanza per la sicurezza dei sistemi informatici e conseguentemente per la sicurezza delle informazioni personali a cui potrebbero accedere nello svolgimento dei propri compiti.

La presente Politica recepisce i requisiti definiti nel provvedimento del Garante per la protezione dei dati personali (di seguito Garante Privacy o Garante) del 27/11/2008 *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema"*.

Il Provvedimento del Garante Privacy sugli Amministratori di Sistema prevede specifiche accortezze che devono essere adottate nella designazione e gestione degli Amministratori di Sistema, prevedendo nello specifico, attività di verifica sull'operato di questi ultimi per garantire la conformità alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle normative vigenti.

L'ACSS, nella persona del Titolare del trattamento dei dati personali (di seguito Titolare), recepisce ed include la presente Politica nell'insieme delle misure di carattere organizzativo e procedurale che concorrono alla tutela dei diritti dell'interessato ed alla sicurezza dei dati personali, in ottemperanza al principio di responsabilizzazione, formulato nel Regolamento (UE) 2016/67 (di seguito anche GDPR).

1. INTRODUZIONE

ART 1) SCOPO DEL DOCUMENTO

1. Il presente documento ha lo scopo di definire i requisiti che la ACSS deve recepire e adottare, al fine di assicurare la conformità dell'operato degli Amministratori di Sistema, alle prescrizioni del Provvedimento del Garante Privacy del 27/11/2008, in relazione a tutti i sistemi ICT che trattano dati personali della ACSS.
2. Le regole descritte nella presente Politica sono da considerarsi come misure minime la cui attuazione si rende necessaria per contenere, entro limiti accettabili, il rischio di compromissioni della riservatezza, integrità e disponibilità delle risorse informative della ACSS. In tal senso, queste costituiscono i requisiti di base minimi ed obbligatori che, in

quanto tali, in virtù delle specifiche caratteristiche del contesto operativo a cui si applicano, possono essere incrementati qualora, in determinati contesti, siano richiesti livelli di protezione più elevati.

ART 2) CAMPO DI APPLICAZIONE

1. Le regole descritte nel presente documento, si applicano all'operato degli Amministratori di Sistema che a vario titolo operano sui sistemi ICT della ACSS che trattano dati personali ai sensi del GDPR.
2. In particolare, il ruolo di Amministratore di Sistema si individua all'interno della SC Analisi e sviluppo Sistemi di Controllo di ACSS per le attività di application administrator e credential administrator.

Mentre viene svolto nell'ambito del fleet management, quindi, il ruolo di system administrator, database administrator, network administrator, security administrator, backup/storage e Recovery administrator.

Le specifiche di ciascun ruolo sono esplicitate nell'art. 5, comma 2.

ART 3) DEFINIZIONI E ACRONIMI

1. Ai fini dell'applicazione della presente Politica devono intendersi le seguenti definizioni:
 - a. **Amministratore di Sistema:** soggetto appositamente designato ai sensi del Prov. del Garante Privacy con provvedimento formale della ACSS, alla gestione e/o alla manutenzione dei sistemi informatici della ACSS che trattano dati personali.
 - b. **Collaboratore esterno:** persona fisica che collabora con la ACSS in forza di un contratto libero professionale.
 - c. **Dato Personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
 - d. **Estremi identificativi degli Amministratori di Sistema:** si tratta del minimo insieme di dati identificativi utili a individuare il soggetto nell'ambito dell'Organizzazione di appartenenza. In molti casi possono coincidere con nome, cognome, funzione o area organizzativa di appartenenza.
 - e. **Personale:** dipendente o assimilabile (es. contratti atipici).
 - f. **Responsabile del Trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che tratta i dati personali per conto del titolare del trattamento.
 - g. **Risorse Informative:** i dati, le informazioni, le risorse informatiche, i supporti digitali e cartacei di archiviazione.

- h. **Soggetti terzi:** Fornitori, consulenti, collaboratori esterni, partner che operano con la ACSS in forza di un contratto.
 - i. **Titolare del Trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che singolarmente o insieme ad altri, determina le finalità e i mezzi per il trattamento dei dati personali.
 - j. **Trattamento:** qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
 - k. **Utente:** persona fisica che utilizza un'applicazione/sistema ICT.
 - l. **Utenza:** credenziali di autenticazione (o user account) utilizzate dagli utenti per l'accesso ai sistemi ICT.
 - m. **Utenza Amministrativa:** utenza nominale con diritti di accesso privilegiati assegnata agli Amministratori di Sistema, con riferimento al Prov. del Garante Privacy del 27 /11/2008 e s.m.i.
3. Ai fini dell'applicazione della presente Politica devono intendersi i seguenti acronimi:
- a. **ACSS:** Agenzia di Controllo del sistema Sociosanitario lombardo.
 - b. **C.P.:** Codice penale.

2. ETICA E COMPORTAMENTI SANZIONATI DALLE NORMATIVE VIGENTI

ART 4) ETICA E COMPORTAMENTI SANZIONABILI

1. La ACSS consapevole che l'etica nei comportamenti costituisce valore e condizione di successo della propria missione e che principi quali la trasparenza, l'affidabilità e il senso di responsabilità rappresentano la base fondamentale di tutte le attività che caratterizzano la sua funzione istituzionale, definisce le linee guida a cui sono improntati i comportamenti nelle relazioni interne e nei rapporti con l'esterno. È importante, dunque, essere consapevoli che l'attuazione di alcuni comportamenti, oltre a non configurarsi eticamente corretta, rappresenta anche un illecito e quindi perseguibile nell'ambito dell'ordinamento giuridico italiano.
2. Nello specifico contesto della presente Politica, il ruolo di Amministratore di Sistema può costituire un'aggravante in alcuni reati penali di seguito elencati:
 - a. accesso abusivo a sistema informatico o telematico (art. 615 ter del c.p.);
 - b. frode informatica (art. 640 ter del c.p.);

- c. danneggiamento di informazioni, dati e programmi informatici (artt.635 bis e ter del c.p.);
 - d. danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinquies del c.p.).
3. La mancata applicazione di quanto espresso nella presente Politica, può inoltre esporre la ACSS a possibili sanzioni derivanti dall'inadempienza alle misure cogenti.

3. RUOLO DI AMMINISTRATORE DI SISTEMA

ART 5) DESCRIZIONE

1. In assenza di definizioni normative e tecniche condivise, nell'ambito del Provvedimento del Garante Privacy, l'Amministratore di Sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali. Non rientrano nella definizione, quei soggetti che solo occasionalmente, intervengono per esempio a scopo di manutenzione a seguito di guasti o malfunzionamenti, sui sistemi di elaborazione e sui sistemi software.
2. Ai fini del presente documento, e in linea con quanto previsto dal Provvedimento del Garante Privacy, si considerano Amministratori di Sistema le figure professionali che ricoprono uno o più dei seguenti ruoli, indipendentemente dalla tipologia di dati personali trattati:
 - a. **system administrator**, ruolo attribuito agli operatori preposti alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (sistemi informatici, server, apparati hardware, inclusi sistemi operativi);
 - b. **database administrator**, ruolo attribuito agli operatori preposti alla gestione della struttura logica, delle attività di ottimizzazione delle prestazioni ed in genere del middleware costituito dai Data Base Management System;
 - c. **application administrator**, ruolo attribuito agli operatori preposti alla gestione di applicazioni (software, applicazioni, siti web);
 - d. **network administrator** ruolo attribuito agli operatori preposti alla gestione delle reti informatiche di comunicazione e dei relativi apparati;
 - e. **security administrator**, ruolo attribuito agli operatori preposti alla gestione delle componenti/apparati e delle piattaforme hardware e software dedicate alla sicurezza dei sistemi informatici e delle reti;

- f. **backup/storage e Recovery administrator:** ruolo attribuito agli operatori che gestiscono i supporti di memorizzazione e le attività di back-up/restore dei sistemi hardware e software e delle basi di dati;
- g. **credential administrator:** ruolo attribuito agli operatori preposti alla gestione delle credenziali di autenticazione e alla gestione dei permessi di accesso ai sistemi informatici.

4. GESTIONE DEGLI AMMINISTRATORI DI SISTEMA

ART 6) REQUISITI GENERALI

1. Sono di seguito sintetizzati i requisiti di attuazione delle prescrizioni contenute nel Provvedimento del Garante Privacy in relazione agli Amministratori di Sistema:
 - a. **valutazione delle caratteristiche soggettive:** *l'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;*
 - b. **designazione individuale dell'Amministratore di Sistema:** *l'attribuzione dell'incarico di Amministratore di Sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;*
 - c. **gestione dell'elenco degli Amministratori di Sistema:** *l'elenco degli estremi identificativi delle persone fisiche Amministratori di Sistema, con l'ambito di operatività ad essi attribuito, deve essere mantenuto aggiornato e disponibile in caso di accertamenti da parte del Garante Privacy;*
 - d. **registrazione degli accessi degli Amministratori di Sistema:** *devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di Sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;*
 - e. **servizi in outsourcing:** *nel caso di servizi di gestione in outsourcing il fornitore dovrà fornire, su richiesta della ACSS nella persona del Titolare del trattamento, gli estremi identificativi delle persone fisiche che svolgono il ruolo di Amministratori di Sistema in ottemperanza al servizio erogato;*
 - f. **verifica delle attività:** *l'operato degli Amministratori di Sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare del trattamento, o di persone da lui incaricate, in modo da controllare l'osservanza delle*

misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali.

ART 7) REQUISITI PER LA VALUTAZIONE DELLE CARATTERISTICHE SOGGETTIVE

1. Prima della designazione ad Amministratore di Sistema, devono essere valutate attentamente le caratteristiche soggettive quali esperienza, capacità e affidabilità, con riferimento a qualità tecniche, professionali e di condotta, dei soggetti da designare, che devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza.
2. i soggetti da designare quali Amministratori di Sistema, è inoltre richiesta la conoscenza e l'accettazione delle disposizioni vigenti in materia di trattamento dei dati personali e delle norme per la sicurezza delle informazioni, con particolare riferimento a:
 - a. conoscenza delle normative di leggi applicabili;
 - b. conoscenza delle politiche interne alla ACSS, nonché delle best practice di riferimento in materia di gestione "sicura" dei sistemi informatici;
 - c. consapevolezza dei rischi di sicurezza derivanti da errori, omissioni e violazioni delle regole applicabili allo svolgimento delle attività di Amministratore di Sistema.
3. Il processo di valutazione delle caratteristiche soggettive in caso di servizi di amministrazione dei sistemi ICT affidati a soggetti terzi (outsourcing), è in carico a questi ultimi. Tali valutazioni possono in ogni momento essere verificate e validate dal Titolare della ACSS o da persone da questo incaricate.

ART 8) REQUISITI PER LA DESIGNAZIONE INDIVIDUALE

1. L'attribuzione dell'incarico di Amministratore di Sistema, deve essere in ogni caso individuale, ossia la persona designata deve essere identificabile in maniera univoca. A tale scopo, la ACSS, nella persona del Titolare, predispone una lettera di incarico, che deve contenere le seguenti informazioni:
 - a. elencazione analitica degli ambiti di operatività consentiti, in base al profilo di autorizzazione assegnato, evitando l'attribuzione di ambiti insufficientemente definiti (es. occorre specificare l'ambito di operatività per settori o per aree applicative o specificare i singoli sistemi, laddove necessario);
 - b. notifica che l'operato dell'Amministratore di Sistema può essere soggetto a verifiche con cadenza perlomeno annuale, anche attraverso la rilevazione e la successiva analisi dei log di accesso (login, logout, tentativi di accesso) generati sui sistemi ICT nel corso dello svolgimento delle attività di amministrazione;
 - c. notifica che la nomina ed il relativo nominativo potrebbero essere comunicati al personale della ACSS ed eventualmente a terzi nei modi previsti dalle vigenti leggi,

qualora la sua attività abbia a riferimento sistemi ICT sui quali sono presenti dati personali afferenti al personale della ACSS o sia nelle condizioni di acquisire conoscenza di dati a essi riferiti (cfr. comma 3 dell'Art. 9).

2. La lettera di nomina ad Amministratore di Sistema deve essere firmata per accettazione dalla persona designata, e opportunamente conservata da parte delle funzioni competenti individuate nell'ambito della ACSS.
3. Il processo di designazione, in caso di servizi di amministrazione dei sistemi ICT affidati a soggetti terzi (outsourcing), è in carico a questi ultimi.

ART 9) REQUISITI PER LA GESTIONE DELL'ELENCO DEGLI AMMINISTRATORI DI SISTEMA

1. L'elenco degli Amministratori di sistema deve contenere le seguenti informazioni:
 - a. gli estremi identificativi delle persone fisiche designate, la cui attività riguarda, anche indirettamente, servizi o sistemi che trattano o che permettono il trattamento di dati personali;
 - b. l'elenco delle funzioni operative ad essi attribuite.
2. L'elenco contenente gli estremi identificativi del personale della ACSS designato Amministratore di Sistema e l'ambito di operatività ad essi attribuito, deve essere mantenuto aggiornato e disponibile in caso di accertamenti da parte del Garante Privacy. L'elenco deve essere aggiornato in occasione di nuove nomine o modifiche/revoche degli incarichi. A tal fine queste ultime devono essere prontamente segnalate alla SC Analisi e Sviluppo Sistemi di controllo, quale Unità Organizzativa della ACSS incaricata della gestione dell'elenco. In ogni caso, almeno una volta l'anno deve essere effettuata la revisione della correttezza delle informazioni riportate nell'elenco.
3. Il Titolare è inoltre tenuto ad instaurare un regime di conoscibilità dell'identità degli amministratori di sistema, quale forma di trasparenza interna alla ACSS a tutela dei lavoratori (ad esempio tramite strumenti di comunicazione interna come la intranet aziendale, ordini di servizio a circolazione interna o bollettini), nel caso in cui un Amministratore di Sistema, oltre a intervenire sotto il profilo tecnico in generici trattamenti di dati personali per la ACSS, tratti anche dati personali riferiti ai lavoratori operanti nell'ambito dell'organizzazione medesima o sia nelle condizioni di acquisire conoscenza di dati a essi riferiti. Tale forma di pubblicità o conoscibilità non si attua qualora vi sia una disposizione di legge che ne impedisca l'utilizzo.
4. In caso di servizi di amministrazione dei sistemi ICT affidati a soggetti terzi (outsourcing), la gestione dell'elenco di tali Amministratori di Sistema è in carico ai soggetti terzi. Questi ultimi devono comunicare tale elenco all'ACSS, al verificarsi delle seguenti condizioni:

- a. avvio del contratto di fornitura;
- b. nuove nomine o modifiche/revoche degli incarichi precedentemente comunicati;
- c. richiesta da parte del Titolare della ACSS o persone da questo delegato.

ACSS detiene il registro per le attività di cui è Amministratore di sistema.

ART 10) REQUISITI PER LA REGISTRAZIONE DEGLI ACCESSI

1. Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi elettronici ed agli archivi informatici da parte degli Amministratori di Sistema (log di accesso), con particolare riferimento agli accessi (login), alle disconnessioni (logout) e ai tentativi di accesso effettuati dagli amministratori di sistema nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software (es. sistemi operativi, middleware, apparati di rete, apparati di sicurezza, sugli applicativi complessi, sui dispositivi di memorizzazione).
2. Le registrazioni (log di accesso) di cui al comma precedente, devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo per cui sono state richieste.
3. La caratteristica di **completezza** è riferita all'insieme degli eventi censiti nel sistema di log, che deve comprendere tutti gli eventi di accesso interattivo, e tentativi di accesso, generati dalle attività degli Amministratori di Sistema su tutti i sistemi precedentemente indicati. Le registrazioni devono inoltre comprendere, i riferimenti temporali e la descrizione dell'evento che le ha generate.
4. Le caratteristiche legate al mantenimento dell'**inalterabilità** dei dati raccolti dai sistemi di log, sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito software. Il requisito può essere ragionevolmente soddisfatto con la strumentazione software in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei log di accesso su supporti di memorizzazione non riscrivibili, ai fini della relativa conservazione. In casi più complessi è possibile adottare sistemi più sofisticati quali piattaforme centralizzate per la gestione dei log con l'utilizzo di canali di trasmissione sicuri.
5. La caratteristica legata alla possibilità di **verifica dell'integrità** dei log può essere soddisfatta, ad esempio, tramite l'applicazione di tecniche di cifratura, timestamping ed hashing.
6. I log di accesso ai sistemi di elaborazione e agli archivi elettronici effettuati dagli Amministratori di Sistema, devono essere conservati per un congruo periodo, non inferiore a sei (6) mesi. Trascorso tale periodo, dovrà esserne prevista la cancellazione definitiva da ogni sistema ICT e/o supporto di archiviazione.

7. Devono essere pertanto implementate idonee soluzioni tecnologiche atte a garantire la creazione e la raccolta dei log di accesso degli Amministratori di Sistema, secondo le caratteristiche di completezza, inalterabilità e verifica della loro integrità definite nella presente Politica.
8. In caso di servizi di amministrazione dei sistemi ICT affidati a soggetti terzi (outsourcing), le soluzioni tecniche di cui al precedente comma 8, possono essere adottate dal Titolare e/o dal soggetto terzo in funzione del contesto tecnologico di riferimento e della modalità di erogazione del servizio da parte del soggetto terzo. L'effettiva adozione ed efficacia delle eventuali soluzioni adottate dal soggetto terzo possono in ogni momento essere verificate e validate dal Titolare della ACSS o da persone da questo incaricate.

ART 11) REQUISITI PER LA VERIFICA DELLE ATTIVITÀ

1. Devono essere effettuate verifiche periodiche sull'operato degli Amministratori di Sistema, con cadenza almeno annuale, per rilevarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali. Di seguito sono descritte le attività di verifica, con un'indicazione di massima sulla rispettiva cadenza periodica:
 - a. **cadenza annuale:** verifiche di riscontro, su un campione significativo di sistemi ICT, della corretta generazione dei log di accesso, della loro conformità e della conservazione sicura degli stessi per almeno sei mesi, coerentemente con quanto previsto dal Provvedimento del Garante Privacy (cfr. Art. 10);
 - b. **cadenza annuale:** analisi di dettaglio dei log di accesso, su un campione significativo di sistemi ICT, al fine di riscontrare eventuali anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso, postazioni di lavoro utilizzate, ecc.);
 - c. **cadenza annuale:** verifiche di riscontro dell'attuazione del processo di gestione dell'elenco degli Amministratori di Sistema e verifica dell'allineamento di tale lista, con l'assegnazione dei ruoli e dei relativi ambiti di operatività (cfr. Art. 8 e Art. 9);
 - d. **su richiesta:** ogni qualvolta vi sia necessità interna o su richiesta degli organi esterni (es. Autorità Giudiziaria, Garante Privacy), di effettuare attività di controllo specifiche.
2. Le suddette attività di verifica devono essere formalizzate in un report denominato "Rapporto di verifica delle attività svolte dagli Amministratori di sistema", attestante:
 - a. la data di esecuzione delle attività;
 - b. l'ambito di applicazione delle verifiche effettuate (sistemi informatici e tipologie di log);
 - c. le tipologie di verifiche compiute ed i relativi esiti;
 - d. le eventuali non conformità, anche parziali e le eventuali raccomandazioni per il miglioramento;

- e. l'eventuale Action Plan a fronte di non conformità rilevate, con la chiara indicazione della responsabilità per l'esecuzione e la verifica delle attività (action) previste nonché delle tempistiche entro le quali completare tali attività;
 - f. la responsabilità della verifica dell'attuazione dell'Action Plan.
3. In caso di servizi di amministrazione dei sistemi ICT affidati a soggetti terzi (outsourcing), il Titolare è responsabile dell'attuazione del requisito di verifica sulle attività degli Amministratori di Sistema (cfr. Art. 11), anche se l'attuazione di tale adempimento può essere formalmente demandata al soggetto terzo.

ART 12) REQUISITI CONTRATTUALI PER LA GESTIONE DEI SERVIZI DI AMMINISTRAZIONE DI SISTEMA DA PARTE DI SOGGETTI TERZI (OUTSOURCING)

1. In caso di servizi di amministrazione dei sistemi ICT affidati a soggetti terzi (outsourcing), questi ultimi devono essere nominati Responsabili del Trattamento ai sensi dell'art. 28 del GDPR e l'obbligo di assolvimento delle prescrizioni contenute nella presente Politica deve essere esplicitato nell'accordo di designazione e nelle clausole contrattuali afferenti al servizio erogato.

5. DOCUMENTI DI RIFERIMENTO

1. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – Garante Privacy – Provvedimento del 27/11/2008 e s.m.i.
2. Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento del 25/06/2009
3. Regolamento (UE) 2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone con riguardo al trattamento dei dati personali – Regolamento Generale sulla Protezione dei Dati (GDPR) e s.m.i.
4. D.lgs. 101/2018: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
5. Legge n.547 del 23 dicembre 1993 sul tema della criminalità informatica
6. Codice penale dello Stato italiano
7. Modello Organizzativo Data Protection della ACSS
8. Politica per la Sicurezza delle informazioni della ACSS

POLITICA SPECIFICA PER LA GESTIONE DELLE UTENZE

Una corretta gestione delle utenze che accedono ai sistemi informatici dell'ACSS contribuisce, insieme alle altre misure di sicurezza adottate, a garantire la riservatezza, l'integrità e la disponibilità delle Risorse Informative dell'ACSS.

Tale gestione si rende necessaria anche ai sensi di quanto previsto dalla Direttiva NIS 2016/1148 e dal principio di responsabilizzazione formulato nel Regolamento (UE) 2016/67 (di seguito anche GDPR).

La ACSS recepisce ed include la presente politica nell'insieme delle misure di carattere organizzativo e procedurale previste dalla Politica per la Sicurezza delle informazioni della ACSS, a protezione dei dati ed a tutela dei diritti dell'interessato.

1. INTRODUZIONE

ART 13) SCOPO DEL DOCUMENTO

1. L'obiettivo del presente documento è quello di definire le regole per la gestione delle credenziali di accesso (nel seguito anche utenze) degli utenti che accedono ai sistemi informatici dell'ACSS.

2. Le regole descritte all'interno del presente documento sono da considerarsi misure minime la cui attuazione si rende necessaria per contenere, entro limiti accettabili, il rischio di compromissioni della riservatezza, integrità e disponibilità delle informazioni trattate dai sistemi informatici, derivanti da accessi impropri e/o non autorizzati. In tal senso, tali regole costituiscono i requisiti minimi ed obbligatori che, in quanto tali, in virtù delle specifiche caratteristiche del contesto operativo a cui si applicano, possono essere incrementati qualora, in determinati contesti, siano richiesti livelli di protezione più elevati.

ART 14) CAMPO DI APPLICAZIONE

3. Il presente documento si applica a tutte le utenze e a tutti i sistemi/servizi informatici della ACSS.

ART 15) DEFINIZIONI E ACRONIMI

4. Ai fini dell'applicazione della presente Politica devono intendersi le seguenti definizioni:

Amministratore di Sistema: soggetto appositamente designato ai sensi del Provv. del Garante Privacy con provvedimento formale, alla gestione e/o alla manutenzione dei sistemi informatici della ACSS che trattano dati personali.

At least privilege: principio di sicurezza secondo il quale ad un Utente viene concesso il privilegio minimo indispensabile che consente il livello di accesso necessario a svolgere le attività lavorative di sua competenza.

Autenticazione forte o Strong Authentication: si tratta di una procedura informatica per convalidare l'identificazione di un Utente basata sull'uso di due o più elementi di autenticazione, appartenenti ad almeno due categorie tra le seguenti: *conoscenza* (qualcosa che solo l'utente conosce, come una password o un PIN); *possesso* (qualcosa che solo l'utente possiede, come un token/chiavetta, o uno smartphone); *inerenza* (qualcosa che caratterizza l'utente, come l'impronta digitale o il riconoscimento facciale). Questi elementi devono essere indipendenti tra loro, in modo che un'eventuale violazione di uno di essi non comprometta l'affidabilità degli altri.

Collaboratore esterno: persona fisica che collabora con la ACSS in forza di un contratto libero professionale.

Credenziali di accesso o di autenticazione: l'insieme degli elementi identificativi di un Utente.

Dato Personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Need to know: principio di sicurezza secondo il quale ad un Utente sono concessi i privilegi di accesso alle risorse informatiche, in ragione del ruolo organizzativo e in più generale della necessità, derivante dal proprio incarico in seno all'Organizzazione, di accedere ai suddetti sistemi.

Password: sequenza di caratteri alfanumerici e/o speciali tenuta segreta e necessaria per autenticarsi ad un sistema informatico o ad un applicativo.

Personale: dipendente o assimilabile (es. contratti atipici).

Risorse informative: Cfr. Art.2 comma 4 della *Politica per la Sicurezza delle Informazioni della ACSS*.

Soggetti terzi: Fornitori, consulenti, collaboratori esterni, partner che operano con la ACSS in forza di un contratto.

Supporto Informatico: Computer o lo strumento elettronico messo a disposizione dell'Utente, contenente software ed in grado di collegarsi in rete per l'utilizzo dei sistemi informatici e degli applicativi dell'Organizzazione.

User ID: Sequenza alfanumerica che identifica univocamente (generalmente in associazione con una password) l'assegnatario dell'utenza ad un sistema.

Utente: persona fisica che è autorizzata ed abilitata ad accedere alle risorse informatiche.

Utenza: credenziali di accesso assegnate per l'accesso ai sistemi ICT.

Utenza Amministrativa: utenza nominale con diritti di accesso privilegiati assegnata agli Amministratori di Sistema, con riferimento al Prov. del Garante Privacy del 27/11/2008 e s.m.i.

Utenza Amministrativa impersonale: utenza impersonale con diritti di accesso privilegiati, utilizzata per l'amministrazione dei sistemi ICT (es. root, administrator).

Utenza tecnica o di servizio: utenza afferente a processi macchina utilizzata dai programmi informatici (es. application-to-application).

2. ETICA E COMPORTAMENTI SANZIONATI DALLE NORMATIVE VIGENTI

ART 16) ETICA E COMPORTAMENTI SANZIONABILI

1. Tutti gli utenti autorizzati ed abilitati ad accedere alle risorse informatiche della ACSS devono essere consapevoli che l'attuazione di alcuni comportamenti negligenti o non conformi alle politiche interne, oltre a non configurarsi come eticamente corretto, rappresenta anche un illecito e come tale perseguibile nell'ambito dell'ordinamento giuridico italiano.
2. Nello specifico contesto della presente Politica, costituisce un reato la messa in atto di determinati comportamenti configurabili come "crimini informatici", di seguito elencati:
 - accesso abusivo a sistema informatico o telematico (art. 615 ter del c.p.);
 - la detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.).
3. In caso di accertate violazioni delle norme sopra indicate la ACSS potrà provvedere all'immediata inibizione delle credenziali di accesso e degli annessi profili autorizzativi, fermo restando ogni valutazione di carattere disciplinare. A tale proposito si rimanda alla Legge n.547/1993 e a tutte le successive modifiche, integrazioni e nuove leggi emanate in materia.

3. ACCESSO ALLE RISORSE INFORMATICHE

ART 17) REGOLE GENERALI

1. L'accesso alle risorse informatiche della ACSS è subordinato al possesso, da parte dell'Utente, delle relative credenziali di accesso.

2. Gli utenti hanno diritto di accesso limitatamente alle risorse informatiche per le quali sono stati espressamente autorizzati e per gli utilizzi strettamente correlati con le mansioni assegnate.

3. Non è consentito che due o più persone fisiche accedano al sistema informatico, simultaneamente o in maniera differita, utilizzando le medesime credenziali di accesso.

4. GESTIONE DELLE CREDENZIALI DI ACCESSO

ART 18) REGOLE GENERALI

1. Le credenziali di accesso devono avere carattere nominativo ed essere riconducibili ad una persona fisica. Le utenze afferenti a processi macchina utilizzate dai programmi informatici (di seguito utenze tecniche o di servizio), per le quali occorre definire requisiti e misure di sicurezza specifiche, possono avere carattere impersonale, ma devono essere comunque riconducibili ad una persona fisica che ne è responsabile.
2. Le credenziali assegnate a ciascun Utente sono di uso strettamente personale e pertanto:
l'assegnatario è tenuto a custodirle con diligenza e in modo appropriato, al fine di contenere i rischi di accessi non autorizzati, furti, frodi, danneggiamenti derivanti dalla diffusione e/o utilizzo improprio delle credenziali;
non ne è ammesso l'utilizzo da parte di persone diverse dall'assegnatario, né questi può cederle a terzi;
l'assegnatario è responsabile di tutte le operazioni effettuate sui sistemi informatici tramite la propria utenza.
3. Le credenziali di accesso, laddove utilizzate, non possono essere assegnate ad una persona fisica diversa dal primo assegnatario, neppure in tempi diversi.
4. Le credenziali assegnate agli Amministratori di sistema, a parità di sistema informatico acceduto, devono essere diverse da quelle utilizzate dallo stesso assegnatario per l'accesso come semplice utente.
5. Il ciclo di vita delle utenze deve essere strettamente legato allo stato di servizio lavorativo/contratto dei relativi assegnatari che operano nell'ambito della ACSS e in tal senso, occorre definire delle procedure che individuino, in relazione allo stato di servizio dell'assegnatario (assunzione, avvio contratto, dimissione, scadenza contratto, pensionamento, licenziamento, assenza prolungata, cambio mansione, ecc.), le attività e le annesse responsabilità correlate al ciclo di vita delle relative utenze (creazione, disattivazione, sospensione, cambio profilo autorizzativo, ecc.).

6. Qualsiasi utenza di tipo “guest”, creata automaticamente dal sistema informatico, deve essere, ove tecnicamente possibile, disattivata; le utenze di default presenti dopo l’installazione iniziale di un sistema informatico devono essere rinominate o comunque disabilitate se non strettamente necessarie per motivi tecnici. Ove non sia tecnicamente possibile la disattivazione occorre individuare procedure atte a fornire identificazione certa di chi ha acceduto con tali utenze ed in quale lasso di tempo.
7. Gli Amministratori di Sistema possono utilizzare utenze amministrative impersonali (es. root, administrator) per accedere localmente ai sistemi informatici della ACSS (es. attraverso una console di sistema) esclusivamente nei seguenti casi eccezionali:
 - quando non sia disponibile la connettività di rete per l’accesso da remoto ai sistemi informatici da parte degli Amministratori di Sistema mediante le proprie utenze amministrative nominali;
 - per esigenze legate alla manutenzione ordinaria o straordinaria dei sistemi informatici da parte degli Amministratori di Sistema, laddove non sia possibile effettuare tali attività da remoto utilizzando le proprie utenze amministrative nominali.
8. L’utilizzo da parte degli Amministratori di Sistema di utenze amministrative impersonali per l’accesso locale ai sistemi informatici della ACSS, nei casi eccezionali di cui al comma precedente, è subordinato all’adozione di idonee procedure di emergenza atte ad assicurare:
 - l’identificazione certa, anche fisica, dell’Amministratore di Sistema che andrà ad utilizzare l’Utenza amministrativa impersonale;
 - le motivazioni giustificative e lo scopo delle attività che richiedono l’uso dell’Utenza amministrativa impersonale;
 - la registrazione della data e dell’ora di accesso e l’individuazione univoca del sistema/i interessato/i;
 - la registrazione dell’intervallo di tempo (login-logout) durante il quale l’Amministratore di Sistema ha utilizzato l’Utenza amministrativa impersonale;
 - adeguata custodia delle password associate alle utenze amministrative impersonali, volta a garantirne la riservatezza e contestualmente la disponibilità nel momento in cui vi sia la necessità di utilizzarle.

Nel caso in cui non siano previsti ambienti separati per il collaudo e l’esercizio dei sistemi informatici, tutte le utenze utilizzate per le attività di collaudo, devono essere rimosse prima del rilascio in esercizio di tali sistemi.

5. GENERAZIONE DELLE CREDENZIALI DI ACCESSO

ART 19) GENERAZIONE DELLE CREDENZIALI

1. La credenziale di accesso è composta, come minimo, da una UserId e da una password personale, le cui caratteristiche sono descritte nel Cap 1 e 2 del presente Capo.

6. USERID POLICY

ART 20) PRINCIPI GENERALI

1. Lo UserId è univoco e deve essere sempre associato ad una sola persona fisica.
2. Le regole di composizione adottate per la generazione dello UserId devono garantire il soddisfacimento dei requisiti espressi all'Art. 6 della presente Politica. In ACSS è costituito da "nome.cognome"
3. Nel momento in cui l'Utente non ha più diritto o necessità di accedere ai sistemi informatici della ACSS, lo UserId deve essere disattivato e non cancellato, al fine di non consentirne la riassegnazione a persone fisiche diverse, anche in momenti diversi e di permettere eventuali indagini future secondo quanto previsto dalla normativa vigente.

7. PASSWORD POLICY

ART 21) PRINCIPI GENERALI

1. Le regole di seguito descritte per la creazione e la gestione delle password, sono di carattere generale, a prescindere dagli eventuali ulteriori controlli e/o meccanismi specifici implementati in determinati contesti e pertanto devono essere applicate anche alle password di default dei sistemi informatici, salvo ove diversamente specificato.

ART 22) REGOLE SEMANTICHE PER LA COMPOSIZIONE DELLA PASSWORD

1. La lunghezza minima delle password è stabilita in otto caratteri, per gli Amministratori di Sistema la password deve essere costituita possibilmente da almeno quattordici caratteri oppure deve essere utilizzata un'autenticazione forte.

2. Le password devono essere costruite utilizzando caratteri alfabetici, numerici e simboli speciali disponibili con le tastiere di utilizzo comune.

3. Le password devono contenere almeno un carattere alfabetico maiuscolo, un numero ed un carattere speciale.

4. Non è consentito usare una password che:

- sia riconducibile ad un nome proprio di persona o derivante dallo UserId (ad es. identico, inverso, con le lettere raddoppiate, ecc.) o comunque agevolmente riconducibile all'intestatario dello UserId (ad es. matricola, cognome, dati anagrafici, ufficio/funzione di appartenenza);
- sia composta di sole cifre o di una lettera o carattere ripetuto anche più volte o ancora digitata attraverso l'uso della sola barra spaziatrice;
- contenga riferimenti a dati personali (ad es. indirizzo, telefono, codice fiscale, numero della patente, ecc.) o comunque ad altre parole agevolmente riconducibili all'Utente; possano essere lette sia nell'uno che nell'altro verso (ad es. parole o frasi palindrome: ad es. adda, ossesso, esse, ingegni, ecc.);
- sia uguale alle ultime cinque utilizzate o uguale alla precedente tranne che per un carattere.

5. Sono attivi meccanismi di controllo automatico sulla generazione di password sicure.

ART 23) REGOLE PER LA GESTIONE DEL CICLO DI VITA DELLE PASSWORD

1. Gli eventi che caratterizzano il ciclo di vita di una password sono di seguito sintetizzati:

generazione: ad opera della funzione organizzativa preposta all'amministrazione delle utenze;

custodia: ad opera del sistema informatico e dell'assegnatario;

utilizzo: ad opera dell'assegnatario;

scadenza: in automatico o ad opera della funzione organizzativa preposta all'amministrazione delle utenze per decorrenza del periodo di validità;

modifica: ad opera dell'assegnatario.

ART 24) GENERAZIONE DELLE PASSWORD

1. La generazione della prima password deve essere effettuata, dalla funzione organizzativa preposta all'amministrazione delle utenze, in concomitanza con l'attivazione dell'identificativo utente (UserId) ad essa correlato.

2. Nella generazione della prima password, devono essere utilizzate le regole esposte all'Art. 10.

3. La prima password deve essere comunicata, con modalità diverse da quelle utilizzate per l'identificativo utente, solo all'assegnatario di cui si abbia certezza dell'identità; le successive password legate ad operazioni di reset, devono essere gestite in modo analogo.

4. La prima password ha carattere provvisorio e qualora tecnicamente possibile, non attiva alcuna operazione diversa da quelle strettamente necessarie alla sua modifica (cfr. Art. 15) da parte del dell'assegnatario, con una nuova password conforme alle regole esposte nell'Art. 10. Laddove non sia tecnicamente possibile forzare il cambio password in maniera automatica, l'assegnatario è comunque tenuto ad effettuare il cambio password al primo accesso.

ART 25) CUSTODIA DELLE PASSWORD

1. La password di accesso è strettamente personale e non può essere comunicata ad altri soggetti diversi dall'assegnatario, anche se limitatamente a brevi periodi di utilizzo.

2. Non è inoltre consentito all'assegnatario della password di:

- comunicare la password (anche se scaduta) per telefono o altro mezzo a soggetti non autorizzati che si presentano come colleghi, tecnici, supervisori, autorità competenti, ecc.;
- digitare la password davanti ad altri (ad es. colleghi o estranei), anche se si tratta del personale di assistenza tecnica;
- trascrivere la password su dispositivi o supporti cartacei o elettronici (ad es. foglietti apposti sul personal computer, lasciati sulla scrivania o dentro ad un cassetto, file di testo lasciati sul desktop, ecc.). Qualora si rendesse indispensabile una trascrizione di back-up della password (es. password di bios di postazioni di lavoro o altri sistemi), essa dovrà essere autorizzata e gestita da procedure di sicurezza (es. conservazione della password di bios di postazioni di lavoro o altri sistemi, in busta chiusa all'interno di armadi di sicurezza ad accesso limitato), che ne descrivano il flusso di gestione, nonché le relative competenze e le responsabilità.

3. L'assegnatario, qualora avesse anche solo il dubbio che la propria password sia venuta a conoscenza di altri (sospetta compromissione), è tenuto a modificarla e, nei casi previsti, a segnalare la sospetta o accertata violazione alla funzione organizzativa competente.

4. Il sistema informatico deve conservare le password di accesso, in formato non intelligibile, utilizzando algoritmi hash standard sufficientemente robusti per garantire la non reversibilità della codifica. Non è ammessa in alcun caso la custodia in chiaro delle password, all'interno del sistema informatico.

ART 26) SCADENZA DELLE PASSWORD

1. Il periodo massimo di validità della password è stabilito in 90 giorni. Trascorso tale periodo, deve essere immediatamente attuata la procedura di modifica della password oppure in assenza di tale funzionalità automatica, deve esserne disposto il blocco forzato delle

credenziali di accesso (cfr. Art. 19) da parte della funzione organizzativa preposta all'amministrazione delle utenze, fino al compimento delle operazioni di cambio password.

ART 27) MODIFICA DELLE PASSWORD

1. La modifica di una password è consentita esclusivamente all'assegnatario.
2. L'assegnatario modifica la propria password previo inserimento del proprio identificativo utente e della vecchia password. A tal riguardo è possibile prevedere ulteriori procedure aggiuntive finalizzate all'accertamento dell'identità dell'assegnatario, (es. Self Change Password). Anche in caso di modifica della password, valgono le medesime regole di composizione esposte all'Art. 10.
3. È vietata la modifica di una password con una frequenza superiore alle 2 volte al giorno in quanto tale evento potrebbe attivare controlli su presunte violazioni di sicurezza, da parte della funzione organizzativa preposta all'amministrazione delle utenze.
4. Nella modifica della password non è possibile utilizzare una stessa password prima che siano stati effettuati 12 cambi dalla stessa ("Enforce password history"). Pertanto, andranno cambiate 12 password diverse prima di poter riutilizzare la prima.
5. L'assegnatario deve effettuare la modifica della password provvisoria attribuitagli dalla funzione preposta all'amministrazione delle utenze in sede di attivazione o riattivazione dell'utenza, nel più breve tempo possibile.
6. Nel caso in cui la password non possa essere tecnicamente modificabile dall'assegnatario, ma esclusivamente dalla funzione preposta all'amministrazione delle utenze, occorrerà adottare le opportune misure compensative atte a garantire la modifica della password assegnata e la relativa segretezza.

8. GESTIONE DEI PROFILI AUTORIZZATIVI

ART 28) PRINCIPI GENERALI

1. Per Profilo Autorizzativo (o privilegio utente), si intende un insieme di regole, relative ad un servizio/applicazione/sistema, che ne definiscono le modalità di utilizzo da parte degli utenti. Queste regole possono essere espresse nell'insieme di risorse ed attributi, ossia i cosiddetti "ruoli applicativi" (es. Amministratore, Utente, Operatore) che ne regolano l'accesso.
2. I profili autorizzativi devono essere:

- a. definiti sulla base delle specifiche applicazioni informatiche (es. sistemi, apparati di rete) che gli utenti devono utilizzare durante l'attività lavorativa;
- b. in ragione del ruolo ricoperto e limitatamente alle mansioni svolte;
- c. configurati per limitare l'accesso ai soli dati necessari alle finalità dell'attività lavorativa (principi del "at least privilege" e "need to know");
- d. limitati nel tempo in ragione delle effettive necessità lavorative.

3. Il rilascio dei profili autorizzativi deve avvenire attraverso procedure formalizzate. Le procedure devono comprendere il rilascio delle autorizzazioni speciali per il personale tecnico-sistemistico, e di quelle eventualmente temporanee per il personale addetto alle assistenze/manutenzioni.

9. REGISTRAZIONE DELLE USERID AUTORIZZATE

ART 29) PRINCIPI GENERALI

1. Deve essere predisposto un archivio delle utenze autorizzate all'accesso ai sistemi informatici della ACSS, su un supporto elettronico dedicato. Tale archivio deve contenere la lista degli User-ID con associate informazioni relative all'assegnatario, i diritti di accesso e ciclo di vita.
2. A valle della creazione e della modifica delle utenze da parte degli Amministratori di Sistema della funzione organizzativa preposta all'amministrazione delle utenze, dovrà essere conseguentemente aggiornato il suddetto archivio (registro delle utenze), con il dettaglio delle operazioni svolte sulle medesime utenze (es. creazione, modifica, disattivazione).
3. L'accesso all'archivio delle utenze autorizzate deve essere consentito esclusivamente agli utenti autorizzati.

10.DISATTIVAZIONE E BLOCCO DELLE CREDENZIALI

ART 30) DISATTIVAZIONE DELLE CREDENZIALI DI ACCESSO

1. Le credenziali di accesso non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica (es. Utenze tecniche o di servizio e Utenze Amministrative), per le quali devono essere predisposte specifiche procedure operative. La disattivazione, laddove tecnicamente possibile, deve avvenire in maniera automatica.

ART 31) BLOCCO DELLE CREDENZIALI DI ACCESSO

1. L'utenza deve essere bloccata ogni qualvolta si ipotizzi un rischio di accessi illeciti o di compromissione della password, e comunque ogni volta sia necessario per garantire la sicurezza del sistema informatico.
2. Il blocco deve consistere nella sospensione temporanea dell'utenza, in maniera tale da impedire l'accesso ai sistemi informatici utilizzando tali credenziali.
3. La procedura di blocco dell'Utenza deve essere possibile solo da parte degli Amministratori di Sistema della funzione organizzativa preposta all'amministrazione delle utenze.

11.VERIFICA PERIODICA DELLE CREDENZIALI E DELLE AUTORIZZAZIONI

ART 32) PRINCIPI GENERALI

1. Al fine di ridurre le opportunità di modifica o di uso improprio e/o non autorizzato delle informazioni trattate dalla ACSS, devono essere previste procedure formalizzate per la verifica periodica e comunque annuale, della sussistenza delle condizioni per il mantenimento delle utenze e degli annessi profili autorizzativi associati agli utenti abilitati, con particolare attenzione ai profili autorizzativi privilegiati (es. Amministratori di sistema, come declinato nella relativa Politica specifica).
2. I fattori che possono determinare un cambiamento nella definizione dei profili autorizzativi sono generalmente legati, a titolo esemplificativo e non esaustivo, alle seguenti circostanze:
 - a. cambio di ruolo o mutamento delle mansioni svolte dall'assegnatario dell'Utenza;
 - b. mutamenti dello scenario tecnologico dell'infrastruttura tecnologica;
 - c. evoluzione dello scenario normativo di riferimento.

12.DOCUMENTI DI RIFERIMENTO

1. Regolamento UE n. 679/2016 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE – General Data Protection Regulation (GDPR)
2. Lgs.101/2018 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali,

nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

3. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – Garante per la protezione dei dati personali – Provvedimenti a carattere generale – 27/11/2008 e succ. modificazioni
4. Legge n.547 del 23 dicembre 1993 sul tema della criminalità informatica
5. Codice penale dello Stato italiano D.lgs. 65/2018: Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell’Unione” (Attuazione Direttiva (UE) NIS 2016/1148)
6. Linee Guida per gli Operatori di Servizi Essenziali – Autorità NIS-Settore Salute – luglio 2019
7. Modello Organizzativo Data Protection della ACSS
8. Politica per la Sicurezza delle informazioni della ACSS
9. Politica Specifica per gli Amministratori di Sistema della ACSS

POLITICHE PER LA CANCELLAZIONE SICURA E LO SMALTIMENTO DEI SUPPORTI ELETTRONICI

L'ACSS adotta specifiche misure e procedure volte a minimizzare i rischi per la sicurezza delle informazioni connessi sia alle attività di reimpiego/riciclaggio e smaltimento dei rifiuti di apparecchiature elettriche ed elettroniche che memorizzano dati, sia alla distruzione di informazioni su supporto cartaceo.

La presente politica recepisce i requisiti definiti nella *Politica per la Sicurezza delle Informazioni* emanata dalla ACSS e le misure e gli accorgimenti contenuti nel provvedimento del Garante per la protezione dei dati personali (di seguito "Garante Privacy" o "Garante") del 13 ottobre 2008 "*Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali*" e le relative istruzioni.

In particolare, il Provvedimento del Garante prevede idonei accorgimenti e misure volte a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere reimpiegate o riciclate e/o smaltite.

L'ACSS, nella persona del Titolare del trattamento dei dati personali (di seguito Titolare), in coerenza con il proprio modello organizzativo per la protezione dei dati personali, recepisce ed include la presente politica nell'insieme delle misure di carattere organizzativo e procedurale che concorrono alla tutela dei diritti dell'interessato ed alla sicurezza dei dati personali, in ottemperanza al principio di responsabilizzazione, formulato nel Regolamento (UE) 2016/67 (di seguito anche GDPR).

L'ACSS, secondo un approccio risk-based alla cybersecurity e più in generale alla sicurezza delle informazioni, applica i suddetti accorgimenti e misure non solo ai dati personali, ma anche a dati ritenuti critici per la mission dell'organizzazione.

1. INTRODUZIONE

ART 1) SCOPO DEL DOCUMENTO

1. Il presente documento si pone l'obiettivo di definire requisiti specifici per tutelare la sicurezza delle informazioni inerenti a dati personali e dati ritenuti critici da parte della ACSS, quando il supporto (cartaceo o elettronico) che li ospita è destinato al reimpiego oppure allo smaltimento e di assicurare la conformità alle prescrizioni in materia contenute nel Provvedimento del Garante per la protezione dei dati personali del 13/10/2008 e nelle relative istruzioni.
2. Gli indirizzamenti definiti nella presente politica sono da considerarsi come un insieme di misure minime che contribuiscono al contenimento di violazioni dei dati personali (data breach) ed in generale dei dati critici per la ACSS. Tali misure possono essere incrementate nei casi in cui siano richiesti livelli di protezioni più elevati.

ART 2) CAMPO DI APPLICAZIONE

1. Le regole e gli indirizzamenti definiti nel presente documento, sono validi per l'intera ACSS e per i soggetti terzi che sono coinvolti nelle attività di reimpiego/smaltimento e si applicano a tutte le informazioni trattate dalla ACSS o da soggetti terzi per conto della ACSS, relative a dati personali e/o dati critici per la mission istituzionale.

ART 3) DEFINIZIONI E ACRONIMI

1. Ai fini dell'applicazione della presente Politica devono intendersi le seguenti definizioni:
 - a. **Cybersecurity:** l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza.
 - b. **Collaboratore esterno:** persona fisica che collabora con la ACSS in forza di un contratto libero professionale.
 - c. **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (cfr. art. 4 del GDPR).
 - d. **Personale:** dipendente o assimilabile (es. contratti atipici).
 - e. **Recupero:** qualsiasi operazione il cui principale risultato sia di permettere ai rifiuti di svolgere un ruolo utile, sostituendo altri materiali che sarebbero stati altrimenti utilizzati per assolvere una particolare funzione o di prepararli ad assolvere tale funzione, all'interno dell'impianto o nell'economia in generale.
 - f. **Reimpiego:** consiste nelle operazioni che consentono l'utilizzo dei rifiuti elettrici ed elettronici o di loro componenti "allo stesso scopo per il quale le apparecchiature erano state originariamente concepite, compresa l'utilizzazione di dette apparecchiature o di loro componenti successivamente alla loro consegna presso i centri di raccolta, ai distributori, ai riciclatori o ai fabbricanti" (art. 3, comma 1, lett. e), D.lgs. n. 151/2005;
 - g. **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (cfr. art. 4 del GDPR).
 - h. **Riciclaggio:** qualsiasi operazione di recupero attraverso cui i rifiuti sono trattati per ottenere prodotti, materiali o sostanze da utilizzare per la loro funzione originaria o per altri fini, escluso il recupero di energia, escluso il recupero di energia.
 - i. **Rifiuti di apparecchiature elettriche ed elettroniche:** le apparecchiature elettriche o elettroniche che sono rifiuti ai sensi dell'articolo 183, comma 1, lettera a), del decreto legislativo 3 aprile 2006, n. 152, inclusi tutti i componenti, sottoinsiemi e materiali di

consumo che sono parte integrante del prodotto al momento in cui il detentore si disfi, abbia l'intenzione o l'obbligo disfarsene.

- j. **Riutilizzo:** qualsiasi operazione attraverso la quale prodotti o componenti che non sono rifiuti sono reimpiegati per la stessa finalità per la quale erano stati concepiti.
 - k. **Scarto:** operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
 - l. **Smaltimento:** qualsiasi operazione diversa dal recupero anche quando l'operazione ha come conseguenza secondaria il recupero di sostanze o di energia.
 - m. **Soggetti terzi:** fornitori, consulenti, collaboratori esterni, partner che operano con la ACSS in forza di un contratto.
 - n. **Titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (cfr. art. 4 del GDPR).
 - o. **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (cfr. art. 4 del GDPR).
 - p. **Violazione dei dati personali:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (cfr. art. 4 del GDPR).
1. Ai fini dell'applicazione della presente Politica devono intendersi i seguenti acronimi:
- a. **ACSS:** Agenzia di Controllo del Sistema Sociosanitario lombardo.
 - b. **RAEE:** Rifiuti di Apparecchiature Elettriche ed Elettroniche.

2. REQUISITI GENERALI

1. La ACSS deve definire i ruoli, le responsabilità e le modalità operative per la cancellazione e distruzione sicura delle informazioni di cui al comma 1 dell'Art. 2 in base alla tipologia di supporto utilizzato (cartaceo o elettronico), nonché alla eventuale destinazione d'uso del supporto elettronico sul quale sono memorizzate (reimpiego o smaltimento), recependo quanto riportato nel presente documento e quanto disposto dalla ACSS e dalla Regione Lombardia in relazione alla gestione e conservazione dei documenti.

2. La ACSS deve impartire specifiche istruzioni al personale ed ai soggetti terzi per la cancellazione e distruzione sicura delle informazioni in linea con la presente politica.

3. CANCELLAZIONE E DISTRUZIONE SICURA DI INFORMAZIONI SU DISPOSITIVI ELETTRONICI O INFORMATICI

ART 4) MISURE PER IL REIMPIEGO/RICICLAGGIO E LO SMALTIMENTO DI RIFIUTI ELETTRICI ED ELETTRONICI

1. La ACSS deve adottare le opportune misure di sicurezza per prevenire accessi non consentiti alle informazioni di cui al comma 1 dell'Art. 2, memorizzate nelle apparecchiature elettriche ed elettroniche destinate a essere reimpiegate/riciclate o smaltite, secondo quanto indicato nell'Art. 5 e nell'Art. 6 del presente documento.
2. La ACSS deve adottare le particolari cautele riportate nel Titolo III - del presente documento, quando si avvale di soggetti terzi per le attività di reimpiego/riciclo o smaltimento di dispositivi elettronici o informatici su cui sono memorizzate le informazioni di cui al comma 1 dell'Art. 2.

ART 5) REIMPIEGO SICURO DI DISPOSITIVI ELETTRONICI O INFORMATICI

1. Prima del reimpiego o riciclo di dispositivi elettronici o informatici su cui sono memorizzate le informazioni di cui al comma 1 dell'Art. 2, la ACSS deve adottare le seguenti misure tecniche, da attuare a seconda delle circostanze, anche in combinazione tra loro:
 - a. misure tecniche preventive quali la cifratura di singoli file/gruppi di file o la memorizzazione delle informazioni sui dischi rigidi (hard-disk) dei personal computer o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura;
 - b. cancellazione sicura delle informazioni, da attuare utilizzando programmi informatici (quali wiping program o file shredder) che provvedono, una volta che l'utente abbia eliminato dei file da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati;
 - c. formattazione "a basso livello" dei dispositivi di tipo hard disk (low-level formatting-LLF), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del

dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;

- d. demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso). La demagnetizzazione (degaussing) azzerà tutte le aree di memoria elettronica e rende l'apparato inutilizzabile.

ART 6) SMALTIMENTO SICURO DI RIFIUTI ELETTRICI ED ELETTRONICI

1. Prima dello smaltimento di rifiuti elettrici ed elettronici su cui sono memorizzate le informazioni di cui al comma 1 dell'Art. 2, la ACSS deve garantirne l'effettiva cancellazione, anche ricorrendo, in alternativa o in aggiunta alle misure di cui all'Art. 5, a procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di informazioni.
2. La distruzione sicura dei supporti elettrici ed elettronici, ai fini della cancellazione sicura, deve prevedere il ricorso a procedure o strumenti diversi, quali:
 - a. sistemi di punzonatura o deformazione meccanica;
 - b. distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
 - c. demagnetizzazione (degaussing) ad alta intensità.
3. Le procedure di smaltimento sicuro di Rifiuti di Apparecchiature Elettriche ed Elettroniche devono definire le relative modalità tecniche, nel rispetto dei precedenti commi, delle indicazioni del Garante, delle normative ambientali "relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti" e di tutte le altre fonti normative in materia.

4. DISTRUZIONE SICURA DI INFORMAZIONI SU SUPPORTO CARTACEO

ART 7) DISTRUZIONE DI INFORMAZIONI SU SUPPORTO CARTACEO

1. Per la distruzione delle informazioni di cui al comma 1 dell'Art. 2 su supporto cartaceo, la ACSS deve definire apposite procedure in conformità alla presente politica ed a quanto disposto dalla ACSS e dalla Regione Lombardia in relazione allo scarto dei documenti.

2. La distruzione di documenti cartacei contenenti le informazioni di cui al comma 1 dell'Art. 2 deve essere effettuata con modalità che prevedono l'utilizzo di appositi dispositivi per la distruzione dei documenti o in assenza di questi, i documenti devono essere frammentati in modo da non essere più ricomponibili. La modalità deve essere individuata anche in relazione alla numerosità dei documenti, sempre garantendo il principio di non reversibilità dell'operazione, anche avvalendosi di servizi affidati a soggetti terzi.
3. Tutta la documentazione contenente le informazioni di cui al comma 1 dell'Art. 2 non può essere oggetto di procedure di riutilizzo della carta.
4. La ACSS deve adottare le particolari cautele riportate nel Titolo III - del presente documento quando si avvale di soggetti terzi per le attività di distruzione delle informazioni di cui al comma 1 dell'Art. 2 su supporto cartaceo.

5. RISPETTO DELL'AMBIENTE E CONTENIMENTO DEI COSTI

1. Le procedure di distruzione sicura delle informazioni devono garantire il rispetto delle normative ambientali rivolte allo "sviluppo sostenibile", con particolare riferimento alle norme che regolano, a livello nazionale e locale, la gestione dei rifiuti.
2. Devono essere privilegiate le modalità che consentano di contenere i costi di gestione dei rifiuti derivanti da tali attività (ad es. mediante convenzioni con Consorzi di filiera per il recupero degli imballaggi, Fondazioni, Onlus, Associazioni riconosciute). Tali azioni dovranno essere intraprese nel rispetto della normativa sull'ambiente con particolare riferimento a quanto previsto dal D.lgs. 152/06 "Norme in materia ambientale" e senza pregiudizio per la sicurezza delle informazioni o in violazione della normativa in materia di dati personali.

6. REQUISITI SPECIFICI IN CASO DI AFFIDAMENTO DEL SERVIZIO A SOGGETTI TERZI

ART 8) DEFINIZIONE DI ACCORDI CONTRATTUALI

1. In caso di affidamento del servizio di distruzione e/o cancellazione sicura delle informazioni di cui al comma 1 dell'Art. 2 a soggetti terzi, la ACSS deve inserire all'interno degli accordi contrattuali, le seguenti prescrizioni, ove applicabili allo specifico servizio:
 - a. rispetto delle modalità di esecuzione del servizio in linea con la presente politica, garantendo quanto segue:
 - adozione da parte del soggetto terzo di una metodologia per il tracciamento delle operazioni contrattualmente stabilite;

- possibilità da parte della ACSS di supervisionare le operazioni di distruzione/cancellazione al fine di controllarne la regolarità e la conformità a quanto stabilito contrattualmente;
- b. clausole contrattuali relative alla riservatezza delle informazioni trattate nell'ambito del servizio con impegno alla sottoscrizione di un accordo di riservatezza. Tali clausole devono specificare quanto segue:
 - obbligo del soggetto terzo, per sé, per i propri dipendenti e per qualunque ulteriore soggetto terzo di cui si avvarrà per servizi oggetto degli accordi contrattuali, di mantenere la riservatezza in relazione a qualsiasi notizia e/o informazione concernente direttamente o indirettamente il lavoro svolto e/o l'organizzazione, di cui venga a conoscenza nell'esecuzione dei servizi oggetto degli accordi contrattuali;
 - obbligo del soggetto terzo di comunicare immediatamente alla ACSS qualunque evento che abbia violato o posto in pericolo la riservatezza delle informazioni contenute nel materiale cartaceo/informatico da essa ritirato/custodito ai fini dello svolgimento dei servizi oggetto degli accordi contrattuali;
 - obbligo del soggetto terzo di restituire, al termine della prestazione dei servizi, tutto il materiale cartaceo/informatico ritirato e non distrutto e a sottoscrivere apposita dichiarazione attestante di non essere in possesso di alcun documento e/o atto originale o copia dello stesso contenente informazioni di cui al comma 1 dell'Art. 2;
- c. conformità al provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" e relative istruzioni pratiche per la cancellazione sicura;
- d. nomina del soggetto terzo a Responsabile del trattamento in relazione alle specifiche attività di trattamento dei dati personali ai sensi del GDPR;
- e. conformità al provvedimento del Garante per la protezione dei dati personali del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema";
- f. conformità alle normative applicabili, con particolare riferimento a quelle inerenti alla tutela ambientale e dei dati personali;
- g. facoltà della funzione richiedente della ACSS, di fornire ulteriori e specifiche istruzioni al soggetto terzo all'avvio o in corso di esecuzione del servizio tenendo conto di eventuali modifiche normative e dei processi interni.

2. Prima dell'avvio del servizio, devono essere osservate le seguenti prescrizioni:

- a. sottoscrizione di un accordo di riservatezza di cui al comma 1 dell'Art. 8, con indicazione nominativa delle persone coinvolte nell'erogazione del servizio;

- b. sottoscrizione dell'accordo di designazione del soggetto terzo quale Responsabile del trattamento in relazione alla distruzione del materiale cartaceo e/o elettronico contenente dati personali ai sensi dell'art. 28 del GDPR, se sono trattati dati personali;
 - c. invio da parte del soggetto terzo dell'elenco degli Amministratori di Sistema designati e coinvolti nel servizio, se sono trattati dati personali.
- 3. L'accordo di riservatezza di cui al punto a) del precedente comma 2 deve includere i seguenti aspetti:
 - a. elenco nominativo delle persone fisiche, incaricate dal Soggetto terzo dello svolgimento delle attività con indicazione dello scopo ed oggetto delle attività (sintetica descrizione del progetto/servizio/attività e delle informazioni che dovranno essere trattate);
 - b. assenso a che tali attività vengano effettuate, esclusivamente dal gruppo di persone fisiche sopra identificato, sulle componenti del proprio sistema informatico e sulle informazioni strettamente necessarie allo svolgimento dell'incarico assegnato;
 - c. impegno del soggetto terzo a mantenere il più assoluto riserbo ed a trattare in maniera confidenziale, non divulgando e cedendo a terzi in alcun modo, tutte le informazioni di cui possa venire a conoscenza nell'ambito delle attività espletate, in esecuzione del mandato conferito;
 - d. impegno del soggetto terzo a non utilizzare il materiale fornito dal Committente per attività diverse ed al di fuori dall'ambito concordato e di trattarlo osservando i principi di correttezza, proporzionalità e liceità.

ART 9) PRESA IN CONSEGNA/RITIRO DEL MATERIALE

- 1. Il soggetto terzo incaricato del servizio, deve contattare la ACSS per definire i tempi e le modalità dell'intervento prima:
 - a. della presa in consegna del materiale, nel caso in cui l'attività venga svolta presso i locali della ACSS;
 - b. del ritiro del materiale, nel caso in cui l'attività venga svolta fuori dei locali della ACSS.
- 2. Le attività di presa in consegna e/o ritiro devono essere opportunamente tracciate.
- 3. Nel caso di spedizione all'esterno, il materiale oggetto di cancellazione e/o distruzione dovrà essere custodito in plico o sacco chiuso e cautelato, utilizzando strumenti idonei alla tracciatura.

ART 10) CANCELLAZIONE E DISTRUZIONE SICURA

- 1. Il soggetto terzo affidatario del servizio di cancellazione e distruzione sicura delle informazioni di cui al comma 1 dell'Art. 2 su supporto elettronico e/o di distruzione sicura di

tali informazioni su supporto cartaceo deve operare secondo le modalità concordate contrattualmente, in conformità alle normative vigenti ed alla presente politica.

2. La cancellazione e la distruzione sicura delle informazioni di cui al comma 1 dell'Art. 2 possono avvenire presso i locali della ACSS o presso la sede del soggetto terzo, in base a quanto definito contrattualmente.
3. Il soggetto terzo in caso di utilizzo di apparecchiature di demagnetizzazione (degausser) o di distruzione fisica di dispositivi elettronici o informatici deve:
 - a. verificare che i dispositivi di demagnetizzazione siano in grado di azzerare le aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti elettronici che fanno parte del dispositivo e causandone l'inutilizzabilità successiva;
 - b. procedere alla distruzione fisica dei dispositivi di memoria nel caso di supporti ottici a sola lettura (CD-ROM, DVD-R);
 - c. rendere, in alternativa alla demagnetizzazione, gli hard-disk inutilizzabili aprendone l'involucro protettivo e danneggiando meccanicamente le superfici magnetiche (piatti) con l'azione deformante di uno strumento o con appositi punzonatori.
4. Il soggetto terzo deve vigilare sul personale incaricato della procedura di cancellazione o distruzione, al fine di verificare la sicurezza del processo e certificare la chiusura dello stesso, secondo le istruzioni comunicate dalla ACSS, anche con particolare riferimento a:
 - a. la verifica dell'inesistenza o della non intelligibilità delle informazioni di cui al comma 1 dell'Art. 2;
 - b. la formalizzazione delle prassi operative e delle misure tecniche da adottare.
5. Una volta cancellate o distrutte le informazioni, il supporto deve essere smaltito, laddove previsto, secondo le procedure concordate contrattualmente e comunque nel rispetto delle normative cogenti in materia di tutela ambientale.

7. DOCUMENTI DI RIFERIMENTO

1. Regolamento UE n. 679/2016 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE – General Data Protection Regulation (GDPR).
2. D.lgs. 101/2018: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali,

- nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
3. Direttiva 2009/136/CE, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.
 4. Provvedimento del Garante per la protezione dei dati personali del 27/11/2008: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema.
 5. Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008: Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali.
 6. Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori - Scheda informativa del Garante per la protezione dei dati personali del 12 dicembre 2008.
 7. D.lgs. 22/1997: Attuazione delle direttive 91/156/CEE sui rifiuti, 91/689/CEE sui rifiuti pericolosi e 94/62/CE sugli imballaggi e sui rifiuti di imballaggio.
 8. D.lgs. 151/2005: Attuazione delle direttive 2002/95/CE, 2002/96/CE e 2003/108/CE, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti e s.m.i.
 9. D.lgs. 152/2006: Norme in materia ambientale.
 10. D.lgs. 49/2014: Attuazione della direttiva 2012/19/UE sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE).
 11. ISO 9001:2008: Sistemi di Gestione per la Qualità – Requisiti.
 12. ISO/IEC 27001: Tecnologie Informatiche - Tecniche per la Sicurezza - Sistemi di Gestione per la Sicurezza delle Informazioni – Requisiti.
 13. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.
 14. ISO/IEC 27003: Information Technology – Security Techniques – Information security management system implementation guidance.
 15. Modello Organizzativo Data Protection della ACSS.
 16. Manuale di Gestione Documentale – ACSS.
 17. Manuale di Conservazione – ACSS.
 18. Politica per la Sicurezza delle Informazioni – ACSS.
 19. Ruoli e Responsabilità per la Sicurezza delle Informazioni – ACSS.
 20. Manuale della Documentazione Sanitaria e Sociosanitaria – Regione Lombardia.
 21. Titolario e Massimario del Sistema Sanitario e Sociosanitario di Regione Lombardia.
 22. Decreto di Regione Lombardia n. 13455 del 22 settembre 2022 – Regole per i Servizi Infotelematici della giunta regionale.

ORGANIGRAMMA ACSS

