ACSS
AGENZIA DI CONTROLLO DEL SISTEMA SOCIO SANITARIO LOMBARDO

Regione Lombardia

IL COMITATO DI DIREZIONE

DELIBERAZIONE N. 8
DEL 25/10/2023

OGGETTO: APPROVAZIONE DEL REGOLAMENTO PER LA POLITICA DELLA SICUREZZA DELLE INFORMAZIONI E LA CYBER SECURITY DI ACSS

Coordinatore: Giovanni Bladelli
Componente: Loredana Luzzi
Componente: Marino Nonis

L'atto si compone di 130 pagine

di cui 126 di allegato

Il presente documento è sottoscritto con firma digitale e conservato digitalmente secondo la normativa vigente

VISTO il 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);

DATO ATTO che il regolamento suddetto richiede di applicare misure tecniche ed organizzative adeguate, per garantire un livello di sicurezza a sua volta adeguato al rischio per la protezione dei dati personali;

VISTE le seguenti disposizioni:

- D.Lgs. n. 196 del 30 giugno 2003 - Codice in materia di protezione dei dati personali e s.m.i. e Regolamento UE n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 - Regolamento generale sulla protezione dei dati (GDPR);
- 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);
- la Direttiva del Presidente del Consiglio dei Ministri del 1agosto 2015 che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale, alla luce dei crescenti rischi cibernetici che minacciano anche il nostro Paese;
- le Misure minime di sicurezza ICT per le Pubbliche amministrazioni emesse da Agid in attuazione della su indicata Direttiva;
- la Determinazione n. 220/2020 del 17 maggio 2020 - Adozione delle Linee Guida – La sicurezza nel procurement ICT, AgID;
- la 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 ed aggiornata dal Decreto-legge: 14 giugno 2021, n. 82;

RICHIAMATO, in particolare, il Capo III del Regolamento 2016/679 (articoli da 12 a 23) il quale assicura, attraverso la previsione di specifici diritti in capo agli interessati, un elevato livello di tutela;

RICHIAMATE, altresì, le Linee Guida del Gruppo di Lavoro Articolo 29 (sostituito poi dal Comitato europeo per la protezione dei dati) nonché le disposizioni integrative nazionali dettate dal D.lgs. 196/2003, come novellato dal d.lgs. n. 101/2018 e, nella specie, l'articolo 2 undecies che introduce delle limitazioni all'esercizio dei diritti;

RAVVISATA la necessità di definire 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;

EVIDENZIATO che, sulla base della missione istituzionale e del quadro normativo di riferimento, ACSS si pone l'obiettivo di garantire il 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, di quelli legati alla cybersecurity, con particolare riferimento alla salvaguardia:

- della 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;
- dell'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;
- della 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;

VISTO il Regolamento allegato al presente provvedimento quale parte integrante e sostanziale;

PRESO ATTO che il suddetto documento è stato predisposto dal Direttore della SC Analisi e Sviluppo Sistemi di Controllo, con il supporto anche del DPO di ACSS;

A VOTI UNANIMI
DELIBERA

Per i motivi di cui in premessa che qui si intendono integralmente richiamati:

1. di approvare il "Regolamento per la politica della sicurezza delle informazioni e la Cyber Security di ACSS" allegato al presente provvedimento, quale parte integrante e sostanziale;

2. di disporre la pubblicazione del citato Regolamento nella intranet dell'Agenzia;

3. di demandare alle singole strutture dell'Agenzia l'osservanza e l'applicazione del Regolamento;

4. di dare atto che il presente provvedimento non comporta oneri di spesa;

5. di pubblicare il presente provvedimento, immediatamente esecutivo, all'Albo Pretorio on line dell'Agenzia, ai sensi dell'art. 32 della L. n. 69/2009 e dell'art. 17 comma 6 della L.R. n. 33/2009.

Componente Coordinatore
Dott. Giovanni Bladelli

Componente
Dott.ssa Loredana Luzzi

Componente
Dott. Marino Nonis

Regolamento per la Politica della Sicurezza delle Informazioni e la Cyber Security di ACSS

Approvato con:	Deliberazione del Comitato di Direzione
N.:	8
Data:	25.10.2023
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

La mission dell'Agenzia di Controllo del Sistema Sociosanitario lombardo (di seguito ACSS) è quella di promuove 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 Sevizi 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 accettato 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 manutenuti.

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, manutenute 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 ogniqualvolta 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 degradi prestazionali 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'idonea 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 Titolario 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'idonea 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 idonea 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 si 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 RESPONSABILITÁ 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 Facitilities 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'idonea 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'idonea 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 CONTINUITÁ 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 Time 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:

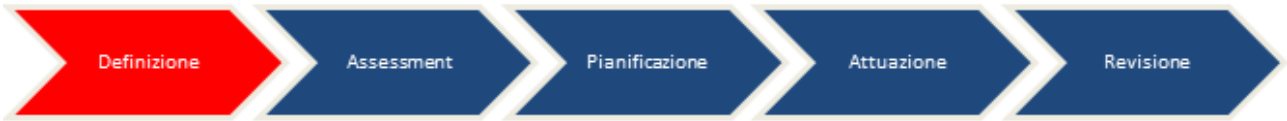
Figura 1 Modello del Sistema di BCM

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, ridurne 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.

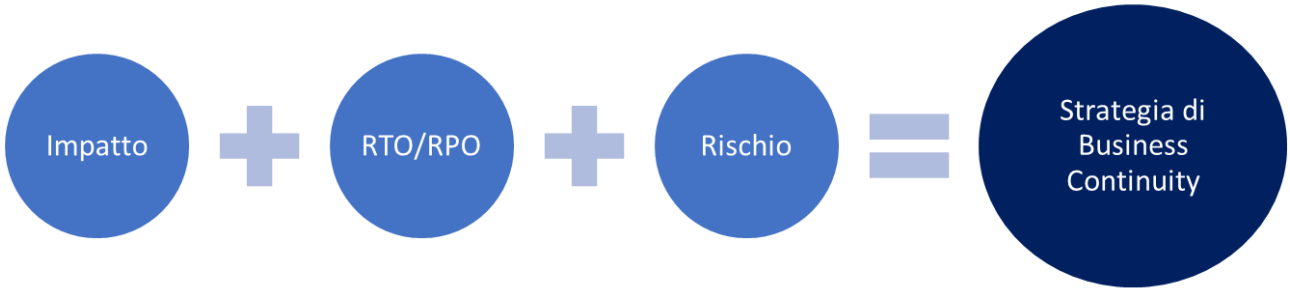


Figura 2 – Strategia di Continuità Operativa

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 CONTINUITÁ 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 Sevizi 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 manutenuta 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 similari) 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 seconde 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 | *Valore non Noto*
Vulnerabilità dell'Asset	Basso | Medio	Basso | Medio	Alto | *Valore non Noto*

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 effettuare 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 ridurne 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 quinques, 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 administratior.
   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 Provv. 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 Provv. 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 quinques 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 Provv. 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 custodita 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, tutti 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 dalla 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 (Raae) 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) azzera 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 (Raae) 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 inserenti 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 si 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 (Raae) 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.