Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

ACSS AGENZIA DI CONTROLLO DEL SISTEMA SOCIO SANITARIO LOMBARDO

Regione Lombardia

Determinazione del Direttore Generale n. 64 del 04/08/2025

OGGETTO

ADESIONE ALL'ACCORDO CONSIP "CYBERSECURITY 2 - ID 2367 – LOTTO 2 PER LA FORNITURA DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI", COD. CUP C41C24000020006

Su proposta della Struttura Complessa:	SC GESTIONE AFFARI ISTITUZIONALI E ATTIVITA' AMMINISTRATIVE PER LE STRUTTURE DI CONTROLLO
Il Direttore responsabile:	Clara Pelliccia
Il Responsabile del procedimento:	Marta Sottoriva
L'istruttore:	Marta Sottoriva
La determinazione del Direttore Generale comporta impegno di spesa:	NO
Attestazione di regolarità economico-contabile: Attestazione non prevista	

IL DIRETTORE GENERALE

PREMESSO che l'art. 11 della L.R. 30/12/2009 n. 33 (Testo Unico delle leggi regionali in materia di sanità), ha istituito l'Agenzia di Controllo del Sistema Sociosanitario Lombardo, quale ente di diritto pubblico dotato di autonomia amministrativa, organizzativa, finanziaria e contabile, organismo tecnico-scientifico;

PRESO ATTO che con DGR n. XII/1651 del 21/12/2023 avente ad oggetto: "Determinazioni in ordine all'Agenzia di Controllo del Sistema Sociosanitario Lombardo (di concerto con l'assessore Bertolaso)" con la quale la dott.ssa Paola Palmieri è stata nominata Direttore Generale di ACSS a far data dal 22/12/2023 sino al termine della Legislatura ai sensi dell'art. 11 della L.R. n. 33/2009, come modificata dalla L.R. n. 22/2021;

VISTA la determinazione del Direttore Generale n. 60 del 27/12/2023 con la quale l'Agenzia di Controllo del Sistema Sociosanitario lombardo ha preso atto della citata DGR;

DATO ATTO che l'Agenzia promuove lo sviluppo e il consolidamento di un sistema di monitoraggio improntato al rafforzamento dei controlli nell'ambito del Sistema Sociosanitario Regionale, a garanzia dell'equità di accesso ai servizi e a tutela del rispetto dei principi di efficienza, efficacia, qualità, trasparenza, appropriatezza ed economicità delle prestazioni e dei servizi erogati;
VISTO il decreto-legge 9 giugno 2021, n. 80 "Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia";
VISTI:

- il decreto-legge del 6 maggio 2021, n. 59, convertito, con modificazioni, dalla legge 1° luglio 2021, n. 101, recante "Misure urgenti relative al Fondo complementare al Piano nazionale di ripresa e resilienza e altre misure urgenti per gli investimenti";
- il decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, recante "Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure" come in ultimo modificato dal decreto-legge 24 febbraio 2023, n. 13 convertito in legge 21 aprile 2023, n. 41, recante "Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e del Piano nazionale degli investimenti complementari al PNRR (PNC), nonché per l'attuazione delle politiche di coesione e della politica agricola comune";
- il decreto-legge 9 giugno 2021, n. 80, convertito con modificazioni, dalla legge 6 agosto 2021, n. 113, recante «Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano

nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia», che definisce percorsi veloci, trasparenti e rigorosi per il reclutamento di profili tecnici e gestionali necessari alle finalità del PNRR, tra cui la cybersicurezza;

- l'art. 47 del citato decreto-legge 31 maggio 2021, n. 77 che ha previsto il rispetto di specifiche clausole negli affidamenti di procedure PNRR in tema di Pari opportunità di genere e generazionali, e il successivo le successive Linee guida "Linee guida volte a favorire la pari opportunità di genere e generazionali, nonché l'inclusione lavorativa delle persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC" adottate con decreto interministeriale del 7 dicembre 2021;
- il Piano Nazionale di Ripresa e Resilienza (di seguito anche "PNRR") - presentato alla Commissione in data 30 giugno 2021 e valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021, notificata all'Italia dal Segretariato generale del Consiglio con nota LT161/21, del 14 luglio 2021 - e, in particolare, le indicazioni contenute relativamente al raggiungimento di Milestone e Target;
- il decreto del Presidente del Consiglio dei ministri del 15 settembre 2021 con il quale sono stati individuati gli strumenti per il monitoraggio del PNRR;
- il decreto ministeriale dell'11 ottobre 2021, recante "Procedure relative alla gestione finanziaria delle risorse previste nell'ambito del PNRR di cui all'articolo 1, comma 1042, della legge 30 dicembre 2020, n. 178";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, 14 ottobre 2021, n. 21, recante "Piano Nazionale di Ripresa e Resilienza Trasmissione alle Amministrazioni centrali dello Stato delle Istruzioni tecniche per la selezione dei progetti PNRR";
- il decreto-legge 6 novembre 2021, n. 152, convertito, con modificazioni, dalla legge 29 dicembre 2021, n. 233, recante "Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, 30 dicembre 2021, n. 32, recante "Piano Nazionale di Ripresa e Resilienza – Guida operativa per il rispetto del principio di non arrecare danno significativo all'ambiente (DNSH)", così come aggiornata con circolare del 13 ottobre 2022, n. 33 ed errata corrige del 24 ottobre 2022;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 31 dicembre 2021, n. 33, recante "Piano Nazionale di Ripresa e Resilienza (PNRR) - Nota di chiarimento sulla Circolare del 14 ottobre 2021, n. 21 - Trasmissione delle Istruzioni Tecniche per la selezione dei progetti PNRR - Addizionalità, finanziamento complementare e obbligo di assenza del c.d. doppio finanziamento";
- il decreto del Presidente del Consiglio dei ministri 15 giugno 2021, recante "Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo

1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133";

- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 21 giugno 2022, n. 27, recante "Piano Nazionale di Ripresa e Resilienza (PNRR) - Monitoraggio delle misure PNRR";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, del 18 gennaio 2022, n. 4, recante "Piano Nazionale di Ripresa e Resilienza (PNRR) - articolo 1, comma 1, del decreto-legge n. 80 del 2021 - Indicazioni attuative";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 24 gennaio 2022, n. 6, recante "Piano Nazionale di Ripresa e Resilienza (PNRR) – Servizi di assistenza tecnica per le Amministrazioni titolari di interventi e soggetti attuatori del PNRR";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 10 febbraio 2022, n. 9, recante "Piano Nazionale di Ripresa e Resilienza (PNRR) - Trasmissione delle Istruzioni tecniche per la redazione dei sistemi di gestione e controllo delle amministrazioni centrali titolari di interventi del PNRR";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, 29 aprile 2022, n. 21, recante "Piano nazionale di ripresa e resilienza (PNRR) e Piano nazionale per gli investimenti complementari - Chiarimenti in relazione al riferimento alla disciplina nazionale in materia di contratti pubblici richiamata nei dispositivi attuativi relativi agli interventi PNRR e PNC";
- il decreto-legge 30 aprile 2022, n. 36, convertito, con modificazioni, dalla legge 29 giugno 2022, n. 79, recante "Ulteriori modifiche urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, del 4 luglio 2022, n. 28, recante "Controllo di regolarità amministrativa e contabile dei rendiconti di contabilità ordinaria e di contabilità speciale. Controllo di regolarità amministrativa e contabile sugli atti di gestione delle risorse del PNRR - prime indicazioni operative";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 26 luglio 2022, n. 29, recante "Circolare delle procedure finanziarie PNRR";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, dell'11 agosto 2022, n. 30, recante "Circolare sulle procedure di controllo e rendicontazione delle misure PNRR", con la quale sono state emanate le "Linee guida di controllo e rendicontazione delle Misure PNRR di competenza delle Amministrazioni centrali e dei Soggetti Attuatori", come aggiornate con circolare del 14 aprile 2023, n. 16 e circolare 15 settembre

2023, n. 27 recante l'adozione della Appendice tematica Rilevazione delle titolarità effettive ex art. 22 par. 2 lett. d) Reg. (UE) 2021/241 e comunicazione alla UIF di operazioni sospette da parte della Pubblica amministrazione ex art. 10, d.lgs. 231/2007;

- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 2 gennaio 2023, n. 1, recante "Controllo preventivo di regolarità amministrativa e contabile di cui al decreto legislativo 30 giugno 2011, n. 123. Precisazioni relative anche al controllo degli atti di gestione delle risorse del Piano Nazionale di Ripresa e Resilienza";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 13 marzo 2023, n. 10, recante "Interventi PNRR. Ulteriori indicazioni operative per il controllo preventivo ed il controllo dei rendiconti delle Contabilità Speciali PNRR aperte presso la Tesoreria dello Stato";
- i principi trasversali previsti dal paragrafo 5.2.1. del PNRR, quali, tra l'altro, il principio del contributo all'obiettivo climatico e digitale (c.d. tagging), il principio di parità di genere e l'obbligo di protezione e valorizzazione dei giovani;
- gli obblighi di assicurare il conseguimento di target e milestone previsti nella Componente e nell'Investimento del PNRR;
- le indicazioni relative al raggiungimento di Milestone e Target contenute negli allegati alla Decisione di esecuzione del Consiglio relativa alla "Approvazione del Piano per la ripresa e la resilienza dell'Italia";
- la Misura M1, Componente C1, Investimento 1.5 del PNRR;
- il target M1C1-19, in scadenza al T4 2024: "Supporto all'aggiornamento delle misure di sicurezza – attivazione di 50 strutture di sicurezza adeguate entro dicembre 2024";
- il Decreto Legislativo 7 marzo 2005, n. 82, recante "Codice dell'Amministrazione Digitale";
- il decreto del Ministro dell'economia e delle finanze del 6 agosto 2021 e ss.mm.ii. relativo all'assegnazione delle risorse in favore di ciascuna Amministrazione titolare degli interventi PNRR e corrispondenti milestone e target che individua la Presidenza del Consiglio dei ministri quale Amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante "Cybersicurezza";
- il 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", che prevede l'istituzione dell'Agenzia a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico;
- l'articolo 7, comma 1, lettere m) e n), del suddetto d.l. n. 82 del 2021 che hanno attribuito all'Agenzia per la Cybersicurezza Nazionale tutte le funzioni in materia di

cybersicurezza già attribuite all'Agenzia per l'Italia digitale e i compiti di cui all'articolo 33-septies, comma 4, del decreto Legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221, nonché la responsabilità di sviluppare "capacità nazionali di prevenzione, monitoraggio, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici […]";

- l'articolo 7, comma 1, lettera t), del suddetto d.l. n. 82 del 2021 che individua l'Agenzia quale autorità che "promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione Europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza nazionale e dei correlati servizi applicativi […]";
- il decreto del Presidente del Consiglio dei ministri del 16 settembre 2021, concernente la "Definizione dei termini e delle modalità del trasferimento di funzioni, beni strumentali e documentazione dal Dipartimento delle informazioni per la sicurezza all'Agenzia per la cybersicurezza nazionale", con il quale il Governo ha definito in favore dell'Agenzia il trasferimento di funzioni, beni strumentali e documentazione anche di natura classificata dal Dipartimento delle informazioni per la sicurezza (DIS);
- le Linee guida per i Soggetti Attuatori versione 3 del 06 marzo 2023 adottate dall'Unità di Missione PNRR del Dipartimento per la trasformazione digitale, Amministrazione Centrale titolare per l'investimento 1.5;

PRESO ATTO che:

- gli investimenti previsti dalla Missione 1 sono declinati in 3 Componenti, tra cui la componente 1 "Digitalizzazione, innovazione e sicurezza della pubblica amministrazione", la quale interviene sugli aspetti di "infrastruttura digitale", spingendo la migrazione al cloud delle amministrazioni, accelerando l'interoperabilità tra gli enti pubblici, snellendo le procedure secondo il principio "once only" e rafforzando le difese di cybersecurity, ed estendendo i servizi ai cittadini, migliorandone l'accessibilità e adeguando i processi prioritari delle Amministrazioni agli standard condivisi a livello europeo;
- con la determina prot. n. 5959 del 26/02/2024 ACN ha approvato l'Avviso Pubblico, avente ad oggetto "Avviso Pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5";
- Ai sensi dell'Avviso sopracitato, sono soggetti attuatori ammissibili – tra gli altri – le Agenzie sanitarie regionali;

DATO ATTO che in data 25/03/2024 l'Agenzia di Controllo ha presentato, su proposta del Direttore della SC Sanità Digitale e Tecnologie Innovative, all'Agenzia per la Cybersicurezza Nazionale – ACN la domanda di ammissione al finanziamento relativo all'avviso Pubblico per il progetto "Attuazione misure tecniche e organizzative in tema di cybersecurity e sicurezza delle informazioni" per un importo complessivo pari a euro 392.000,00;

RICHIAMATA la determinazione n. 04 del 30/01/2025: "Presa d'atto della determina prot. n. unico.0043937.31-12-2024.i adottata dall'Agenzia per la Cybersicurezza nazionale – ACN - relativamente al finanziamento di cui al progetto "avviso pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi comuni, dei comuni capoluogo di regione, delle città metropolitane, delle agenzie regionali sanitarie e delle aziende ed enti di supporto al servizio sanitario nazionale, delle autorità di sistema portuale, delle autorità del bacino del distretto idrografico e delle agenzie regionali per la protezione dell'ambiente a valere sul piano nazionale di ripresa e resilienza, missione 1 – componente 1 –investimento 1.5 "cybersecurity" – codice d'investimento m1c1i1.5"– CUP C41C24000020006 e ulteriori determinazioni;
RICHIAMATA la nota PEC prot. n. 776 del 10/03/2025 con la quale ACSS ha trasmesso al Polo Strategico Nazionale, su proposta del Direttore della SC Sanità Digitale e Tecnologie Innovative un Piano dei Fabbisogni dell'Agenzia, evidenziando due macro-attività relative al trasferimento in sicurezza dell'infrastruttura IT e all'aggiornamento in sicurezza di applicazioni in cloud;

VISTI gli adempimenti previsti dalla Direttiva UE 2022/2555 (NIS 2) che stabiliscono i requisiti principali che le organizzazioni e le pubbliche amministrazioni devono soddisfare per raggiungere un elevato livello di sicurezza informatica;

PRESO ATTO che il Direttore della SC Sanità Digitale e Tecnologie Innovative il 09/07/2025 ha segnalato la necessità, al fine di sviluppare i servizi di cui al finanziamento assegnato con determina prot. n. unico.0043937.31-12-2024.i dall'Agenzia per la Cybersicurezza nazionale di aderire all' Accordo Quadro di Consip S.p.A. "Cybersecurity 2" ID 2367 avente ad oggetto la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le pubbliche amministrazioni, per 24 mesi;

VISTO l'Accordo Quadro di Consip S.p.A. "Cybersecurity 2" ID 2367 avente ad oggetto la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le pubbliche amministrazioni;

PRESO ATTO che il lotto 2 dell'Accordo Quadro di Consip S.p.A. "Cybersecurity 2" ID 2367, d'interesse di ACSS, è stata aggiudicato all'RTI Telecom Italia S.p.A., Maticmind S.p.A., DGS S.p.A., SCAI Solution Group S.p.A.;
DATO ATTO che le modalità di acquisto sono perfezionate con l'emissione dell'Ordinativo Diretto di Acquisto (ODA) e che la sottoscrizione dello stesso implica l'adesione alla convenzione aggiudicata e la conclusione del contratto secondo le condizioni contemplate negli atti di gara predisposti dalla Centrale di Committenza;

PRESO ATTO che:

- in data 18/07/2025 il Direttore della SC Sanità Digitale e Tecnologie Innovative ha trasmesso il piano dei fabbisogni finalizzato alla richiesta all'aggiudicatario del lotto 2, di una soluzione per la fornitura di prodotti d'interesse per ACSS attraverso il rilascio di un piano operativo, nota conservata in atti;
- in data 29/07/2025 il Direttore della SC Sanità Digitale e Tecnologie Innovative, ha fornito parere positivo in relazione al piano operativo ricevuto dal RTI a mezzo PEC in data 24 luglio 2025, e parere favorevole per la prosecuzione delle attività dando seguito alla richiesta attuativa a mezzo portale Consip;
- il piano operativo relativo alla fornitura di prodotti per una Piattaforma di protezione degli endpoint e rilevamento e risposta delle minacce informatiche dannose per ACSS, in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (identificato dal codice: ID 2367 – Richiesta Piano Operativo/Ordine 8646016) ammonta a euro 157.000,00 oltre IVA, per 24 mesi;

DATO ATTO che al fine di perfezionare l'adesione, è necessario approvare il piano operativo, allegato parte integrante della presente determinazione;

RICHIAMATA la DGR n. XII/3720 del 30/12/2024 avente ad oggetto: "Determinazioni in ordine agli indirizzi di programmazione del SSR per l'anno 2025" e, in particolare, l'Allegato 10 "Area investimenti, Acquisti e Internal Auditing";

PRECISATO che:
- a seguito dell'entrata in vigore del decreto legislativo D.lgs. n.31 marzo 2023, n. 36, "Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici" e ai sensi di quanto disposto all'art. 226, comma 2, lett. A del suddetto Decreto Legislativo "a decorrere dalla data in cui il codice acquista efficacia ai sensi dell'articolo 229, comma 2, le disposizioni di cui al decreto legislativo n. 50 del 2016 continuano ad applicarsi esclusivamente ai procedimenti in corso. A tal fine, per procedimenti in corso si intendono le procedure e i contratti per i quali i bandi o avvisi con cui si indice la procedura di scelta del contraente siano stati pubblicati prima della data in cui il codice acquista efficacia";

- la procedura in argomento è stata pubblicata in data antecedente all'entrata in vigore del D.lgs. n.31 marzo 2023, n. 36 e, pertanto, allo stesso si applicano le disposizioni contenute nel D.lgs. n.18 aprile 2016, n. 50;

RICHIAMATA la determinazione n. 43 del 24/05/2024 con la quale ACSS ha approvato il programma triennale degli acquisti di beni e servizi di importo superiore a euro 140.000,00, per gli anni 2024, 2025 e 2026;
RITENUTO di individuare, in coerenza con la determinazione n. 43 del 24/05/2024 succitata, il Dott. Alberto Panese, Direttore della SC Sanità Digitale e Tecnologie Innovative, Responsabile Unico del progetto (RUP), ai sensi dell'art 15 del D.lgs. 36/2023";

RITENUTO altresì di individuare, la dott.ssa Marta Sottoriva quale Responsabile Unico del progetto (RUP) di fase, ai sensi dell'art 15 del D.lgs. 36/2023";

RITENUTO altresì di individuare l'Ing. Frascati Francesca, collaboratore della SC Sanità Digitale e Tecnologie Innovative, quale Direttore dell'esecuzione del contratto, ai sensi dell'art. 114 del D.lgs. n. 36/2023;

RICHIAMATO l'art. 45 del D.lgs. n. 36/2023, il quale prevede che, a valere sugli stanziamenti previsti per le singole procedure, vengano destinate risorse per le funzioni tecniche svolte dai dipendenti in misura non superiore al 2% dell'importo a base delle procedure di affidamento e che tale disposizione si applica anche agli appalti relativi a servizi o forniture nel caso in cui è nominato il direttore dell'esecuzione;

RITENUTO di quantificare, ai sensi dell'art. 45 del D.lgs. n. 36/2023, l'importo di euro 3.145,96 per la costituzione del fondo incentivi per funzioni tecniche che verrà successivamente accantonato secondo le indicazioni regionali in materia;

RICHIAMATA la DGR n. 3855 del 03.02.2025 avente ad oggetto: "Approvazione Bilancio Preventivo Economico 2025";

RITENUTO, pertanto, alla luce di quanto sopra rappresentato, di approvare il piano operativo, procedendo con l'adesione all'accordo quadro di Consip S.p.A. "Cybersecurity 2" ID 2367 avente ad oggetto la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le pubbliche amministrazioni, per 24 mesi per l'importo di 157.298,00 oltre IVA;

RITENUTO altresì di dare mandato al Dirigente Responsabile della SS Bilancio, Programmazione e Acquisti di procedere con la formalizzazione dell'ordine di acquisto sul portale Consip S.p.A., secondo le indicazioni di cui all'Accordo quadro;

PRESO ATTO che la spesa per l'affidamento in parola verrà finanziata con i fondi di cui alla determina prot. n. unico.0043937.31-12-2024.i del 31.12.2024, adottata dall'Agenzia per la Cybersicurezza nazionale – ACN, per un importo pari ad euro 191.903,56, IVA inclusa, giusta determinazione ACSS n. 04 del 30/01/2025;

DATO ATTO che la presente determinazione è conforme ai requisiti richiesti dalla Legge affinché l'atto sia valido (inerente all'agente, all'oggetto, alla forma, alla funzione ed al contenuto) reso dal Responsabile/Direttore della Struttura proponente e dal Direttore o suo delegato della S.C. Gestione Affari Istituzionali e Attività Amministrative per le Strutture di Controllo, per quanto di rispettiva competenza;

DETERMINA

per le motivazioni formulate in premessa che qui si intendono integralmente trascritte:

1. di aderire all'Accordo Quadro di Consip S.p.A. "Cybersecurity 2" ID 2367 avente ad oggetto la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le pubbliche amministrazioni, per 24 mesi, Lotto 2 - ordine diretto - occorrente all'Agenzia di Controllo;

2. di approvare il "Piano Operativo relativo alla fornitura di prodotti per una Piattaforma di protezione degli endpoint e rilevamento e risposta delle minacce informatiche dannose per ACSS", in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (identificato dal codice: ID 2367 – Richiesta Piano Operativo/Ordine 8646016), per l'importo di euro 191.903,56 IVA inclusa, per 24 mesi " ID 2367, lotto n. 2, occorrente a questa Agenzia formulato dall'RTI Telecom Italia S.p.A, Maticmind S.p.A., DGS S.p.A., SCAI Solution Group S.p.A., allegato al presente provvedimento, quale parte integrante e sostanziale;

3. di nominare, il Dott. Alberto Panese, Direttore della SC Sanità Digitale e Tecnologie Innovative, Responsabile Unico del progetto (RUP), ai sensi dell'art. 15 del D.lgs. 36/2023";

4. di individuare, la dott.ssa Marta Sottoriva quale Responsabile Unico del progetto (RUP) di fase, ai sensi dell'art 15 del D.lgs. 36/2023";

5. di individuare l'Ing. Frascati Francesca, collaboratore della SC Sanità Digitale e Tecnologie Innovative, quale Direttore dell'esecuzione del contratto, ai sensi dell'art. 114 del D.lgs. n. 36/2023;

6. di dare mandato al Dirigente Responsabile della SS Bilancio, Programmazione e Acquisti di procedere con la formalizzazione dell'adesione all'Accordo Quadro in parola tramite l'emissione dell'Ordinativo di Fornitura sul MePa per un importo pari ad euro 191.903,56 IVA inclusa;

7. di dare atto che la spesa pari a euro 191.903,56 IVA inclusa, relativa al piano operativo succitato, verrà finanziata con i fondi di cui alla determina prot. n. unico.0043937.31-12-2024.i del 31/12/2024, adottata dall'Agenzia per la Cybersicurezza nazionale – ACN, giusta determinazione ACSS n. 04 del 30/01/2025;

8. di rimandare a successivi provvedimenti l'erogazione dell'incentivo così come disposto dall'art 45 co 2 del 36/2023;

9. di quantificare, ai sensi del co. 2 dell'art. 45 del D.lgs. n.36/2023, l'importo di euro 3.145,96 per la costituzione del fondo incentivi per funzioni tecniche che verrà successivamente accantonato con appositi provvedimenti;

10. di dare atto che il Responsabile del procedimento per l'adozione della presente determinazione è la dott.ssa Marta Sottoriva, Dirigente Responsabile SS Bilancio, Programmazione e Acquisti;

11. di conferire al già menzionato Responsabile ogni più ampia facoltà di attuazione della presente determinazione del Direttore Generale, compresa la diffusione eventuale agli uffici interessati e coinvolti nel presente procedimento;

12. di dare atto che il presente provvedimento è immediatamente esecutivo ed è soggetto alla pubblicazione sull'Albo pretorio Informatico dell'Ente, ai sensi dell'art. 17, comma 6 della L.R. n. 33/2009 e ss. modifiche, con le tutele previste dalla normativa sulla Privacy per i dati personali e particolari ai sensi del Regolamento europeo n. 679/2016/UE e del D.Lgs. n. 196/2003 e s.m.i.

Il Direttore Generale
Paola Palmieri

Il presente documento è firmato digitalmente ai sensi del Codice dell'Amministrazione Digitale

PIANO OPERATIVO PER LA FORNITURA DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT ED EROGAZIONE DI SERVIZI CONNESSI

LOTTO 2

ACSS

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Tabella Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	24/07/2025

Indice

Sommario

1. INTRODUZIONE

1.1 PREMESSA

Il presente documento descrive il Piano Operativo TIM, relativamente alla richiesta di fornitura di prodotti per una Piattaforma di protezione degli endpoint e rilevamento e risposta delle minacce informatiche dannose per ACSS, in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (identificato dal codice: ID 2367 – Richiesta Piano Operativo/Ordine 8646016).

Con questo progetto ACSS ha lo scopo di potenziare la security per l'assetto della sicurezza attuale, con adeguamento alla compliance normativa, la gestione del rischio cyber ed il miglioramento della resilienza aziendale. Intende pertanto acquisire una soluzione EPP/EDR che consente di proteggere gli endpoint di tipo client da minacce quali virus, trojan, worm, etc, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza, nel dettaglio:

Soluzione di EPP e EDR Cynet per 50 endpoint
Servizi di supporto specialistico

1.2 SCOPO

Lo scopo del documento è quello di formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro ed in risposta al Piano dei Fabbisogni inviato dal cliente.

1.3 RIFERIMENTI

Identificativo
Piano dei Fabbisogni - ACSS – Richiesta Piano Operativo/Ordine **8646016**
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Speciale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Generale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato d'oneri
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT –- Offerta Tecnica Lotto Lotti 1,2,3

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

1.4 ACRONIMI E GLOSSARIO

Definizione / Acronimo	Descrizione
AgID	Agenzia per l'Italia Digitale
Consip	Consip S.p.a.
RTI	Raggruppamento Temporaneo d'Impresa

2. ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

Per il coordinamento delle attività contrattuali previste il RTI impiegherà i referenti di seguito indicati:

- ✓ **Responsabile Unico della Attività Contrattuali dell'Accordo Quadro (RUAC-AQ)**

  Nome Cognome: Massimiliano Materazzi
  e-mail: massimiliano.materazzi@telecomitalia.it

che dovrà riferire, per quanto di competenza, a Consip/Organismo Tecnico di Coordinamento e Controllo, ove richiesto, su tutte le tematiche contrattuali relative all'Accordo Quadro.

- ✓ **Responsabile del Fornitore**

  Nome Cognome: Maurizio Tarantino
  telefono/cellulare: 3894466517
  e-mail: maurizio.tarantino@maticmind.it

che riferirà, per quanto di competenza, all'Amministrazione su tutte le tematiche contrattuali relative al Contratto Esecutivo

- ✓ **Referente Tecnico per l'erogazione dei servizi**

  Gianluca Caliò
  telefono/cellulare: 3405148512
  e-mail: Gianluca.Calio@maticmind.it

che dovranno garantire il corretto svolgimento delle attività e dei servizi ed il relativo livello di qualità di erogazione nel rispetto dei KPI previsti dal Capitolato Tecnico – Parte speciale (cfr. capitolo 5).

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

2.1 CATEGORIZZAZIONE DEGLI INTERVENTI

In relazione al Piano Triennale per l'Informatica delle Pubbliche Amministrazioni, di seguito si riporta "l'inquadramento o categorizzazione" degli interventi che l'Amministrazione intende realizzare.

Ambito (layer)	Obiettivi Piano Triennale
□ Servizi	□ Servizi al cittadino
	□ Servizi a imprese e professionisti
	x Servizi interni alla propria PA
	□ Servizi verso altre PA
□ Dati	x Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
	x Aumentare la qualità dei dati e dei metadati
	x Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
□ Piattaforme	□ Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
	Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
	□ Incrementare e razionalizzare il numero di piattaforme per le amministrazioni
□ Infrastrutture	□ Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)
	□ Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud)
	x Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
□ Interoperabilità	□ Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
	□ Adottare API conformi al Modello di Interoperabilità
□ Sicurezza Informatica	x Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
	x Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

3. PROGETTO DI ATTUAZIONE

Il progetto di attuazione prevede la fornitura di quanto indicato nella tabella seguente, in cui viene indicato l'importo contrattuale complessivo; in ciascuna voce oggetto di quotazione economica si indicano il dettaglio dei prodotti e dei servizi oggetto del contratto esecutivo.

Tipologia Prodotto	Codice Articolo	Descrizione Articolo	Produttore	Quantità	Prezzo Totale
Fornitura	CS2L2-EPP-F1-CYN	Fornitura in opera EPP-F1-CYN-Cynet-360-EPP-EDR-C-F1 (Copertura 24 mesi)	Cynet	50	529,50 €
Servizi	CS2L2-SP-STA	Servizio di supporto specialistico - Security Principal - fascia standard	MATICMIND	193	59.830,00 €
Servizi	CS2L2-SSAR-STA	Servizio di supporto specialistico - Senior Security Architect - fascia standard	MATICMIND	159	42.930,00 €
SERVIZI	CS2L2-JSAN-STA	Servizio di supporto specialistico-Junior Security Analyst - fascia standard	MATICMIND	91	20.702,50 €
SERVIZI	CS2L2-SST-STA	Servizio di supporto specialistico-Senior Security Tester - fascia standard	MATICMIND	122	33.306,00 €
Importo Complessivo					**157.298,00 €**

- Gli importi si intendono IVA esclusa

4. PRODOTTI RICHIESTI

PRODOTTI	BRAND	FASCIA	MODELLO	CODICE ARTICOLO PRODUTTORE	N.
FORNITURA	CYNET	1	EPP-F1-CYN	**Cynet-360-EPP-EDR-C-F1**	50

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

5. PRODOTTI DELLA FORNITURA

Nel seguente paragrafo è riportata la descrizione tecnica dei prodotti forniti.

5.1 SOLUZIONE ALL-IN-ONE DI CYNET PER EPP (ENDPOINT PROTECTION PLATFORM) E EDR (ENDPOINT DETECTION AND RESPONSE):

Cynet 360 (AutoXDR) è una piattaforma autonoma e unificata che integra nativamente **EPP + EDR + XDR**, con automazione delle indagini e remediation, supportata da un servizio **MDR 24/7**

EPP – Protezione preventiva

Basata su **Next-Gen Antivirus (NGAV)**: combina firma, AI, analisi comportamentale e static-behavior per bloccare malware, fileless, macro, ransomware, exploit e zero-day.

Include protezioni specifiche:

- **Exploit & Memory Protection**: blocco proattivo delle tattiche di attacco.
- **Device Control** per USB e periferiche.
- **Threat Intelligence**: alimentata da oltre 30 feed IoC
- **Protezione anti-ransomware** con logica dedicata e monitoraggio file/processi
- **Sandboxing**, controllo app/browser, whitelisting e compliance

EDR – Rilevamento e risposta

- Fornisce **monitoraggio continuo** degli endpoint (file, processi, rete, eventi Windows).
- **Analisi avanzata** e correlazione anomalie per scoprire minacce stealth e multi-fase.
- **Deception Technology**: honeyfiles e decoy per catturare i malintenzionati.
- **Visualizzazione attacchi**: mappa del percorso completo e contesto dell'incidente.
- **Playbook automatizzati** per risposte rapide: isolamento, kill process, modifica password, spostamento in AD, integrazione con firewall, script personalizzati.
- **Indagine avanzata** con root-cause analysis, IOCs, forensic e log presenti centralizzati

XDR e MDR

- Cynet unisce EPP+EDR con Network Detection (NDR), User Behavior Analytics e telemetry utente, fornendo un **XDR nativo** su endpoint, rete e utenti.
- Il servizio **CyOps MDR 24/7** monitora, analizza, threat-hunt e migliora protezione continuativa, incluso supporto alla remediation

ESPM – Postura di sicurezza endpoint

- Scansione continua per vulnerabilità e misconfigurazioni (CVE), priorizzazione rischi, report e consigli pratici di mitigazione

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

6.SERVIZIO DI SUPPORTO SPECIALISTICO

Il servizio di Supporto Specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica.
Di seguito si riporta quanto era stato inizialmente richiesto dal cliente nel Piano dei fabbisogni:

Servizio Supporto Specialistico			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (gg/uomo)
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	**81**
Junior Security Analyst - fascia straordinaria	JSAN-STR	JR_SEC_AN_STR	
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	**193**
Security Principal - fascia straordinaria	SP-STR	SEC_PRINC_STR	
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	
Senior Security Analyst - fascia straordinaria	SSAN-STR	SR_SEC_AN_STR	
Senior Security Architect - fascia standard	SSAR-STA	SR_SEC_ARCH_STD	**158**
Senior Security Architect - fascia straordinaria	SSAR-STR	SR_SEC_ARCH_STR	
Senior Security Tester - fascia standard	SST-STA	SR_SEC_TEST_STD	**120**
Senior Security Tester - fascia straordinaria	SST-STR	SR_SEC_TEST_STR	

Per le competenze che ciascuna risorsa specialistica deve possedere si rimanda a quanto previsto nell'allegato 2 – Capitolato Tecnico – Parte Speciale (paragrafo 3.2.4), e come di seguito riportate:

Junior Security Analyst: in possesso di almeno una delle seguenti certificazioni: EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst,

Security Principal: in possesso della certificazione ISACA CISM (Certified Information Security Manager)

Senior Security Architect: in possesso della certificazione (ISC)^2 CISSP (Certified Information System Security Professional)

Senior Security Tester: in possesso di almeno una delle seguenti certificazioni
EC-Council CEH (Certified Etical Hacker) e/o GIAC Penetration Tester e/o Offensive Security Certified Professional e/o CompTIA Pentest+

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Di seguito vengono descritte le attività che l'Amministrazione intende svolgere attraverso il servizio di supporto specialistico:

L'attività di Assesment proposta per l'Agenzia di Controllo del Sistema Sociosanitario Lombardo (ACSS), di seguito "Cliente", ha i seguenti obiettivi principali:

Valutazione dell'assetto di sicurezza attuale: Effettuare una ricognizione sistematica dell'attuale livello di sicurezza informatica e di conformità rispetto ai requisiti del decreto NIS e alle connesse determinazioni ACN. Questa fase fornirà una visione dettagliata delle aree già allineate e delle eventuali lacune da colmare.

Compliance normativa: assicurare il pieno adeguamento al decreto NIS e alle connesse determinazioni ACN, evitando sanzioni e preservando la reputazione. L'assesment fornirà al Cliente una chiara visione del proprio stato di conformità rispetto agli obblighi di legge.

Gestione del rischio cyber: identificare e valutare i rischi cyber cui l'organizzazione è esposta (inclusi quelli legati a terze parti e supply chain), fornendo indicazioni per mitigare vulnerabilità e minacce. Ciò consentirà al Cliente di instaurare un processo continuo di risk management in linea con le best practice, riducendo la probabilità di incidenti e impatti operativi.

Miglioramento della resilienza aziendale: rafforzare la capacità del Cliente di prevenire, rilevare e reagire ad eventi cyber avversi, assicurando la continuità operativa dei servizi essenziali. L'intervento migliorerà la postura di sicurezza complessiva dell'organizzazione, incrementando la resilienza delle infrastrutture tecnologiche e delle procedure interne (es. business continuity, disaster recovery, incident response). Nel complesso, l'assesment supporta il Cliente in un percorso per trasformare gli obblighi NIS2 in un'opportunità di crescita della maturità cyber, integrando la sicurezza nel modello di governance e tutelando gli asset critici dell'organizzazione.

Inoltre, si avvarrà del supporto di figure specialistiche per la gestione dei seguenti temi:

Area formativa e di consapevolezza: Un percorso strutturato di sensibilizzazione e formazione degli utenti. Questo include attività di awareness mirate, simulazioni di phishing periodiche e un onboarding guidato con contenuti formativi personalizzati. Le attività sono supportate dalla gestione operativa e dalla pianificazione di campagne interne, utili a mantenere alta l'attenzione sulle minacce informatiche e ad aumentare la resilienza dell'organizzazione tramite il coinvolgimento attivo del personale.

Tecnologie per la protezione degli endpoint e delle identità: Il cuore della componente tecnologica è basato su una piattaforma integrata che include funzionalità di Endpoint Protection Platform (EPP) e Endpoint Detection and Response (EDR). L'EPP assicura una protezione preventiva contro malware, ransomware, attacchi fileless ed exploit, grazie a motori avanzati basati su analisi comportamentali e intelligenza artificiale. L'EDR, invece, consente il monitoraggio continuo delle attività sugli endpoint e offre strumenti per la detection e risposta a incidenti complessi, attraverso funzioni di isolamento, kill process, rollback e analisi forense.
Accanto a queste funzionalità si integra l'analisi comportamentale degli utenti (User Behavior Analytics – UBA), utile per individuare accessi anomali o movimenti laterali all'interno della rete, e una componente di deception, che implementa trappole digitali (come hx\oneyfiles o honeypots) per intercettare tentativi di intrusione o escalation di privilegi.

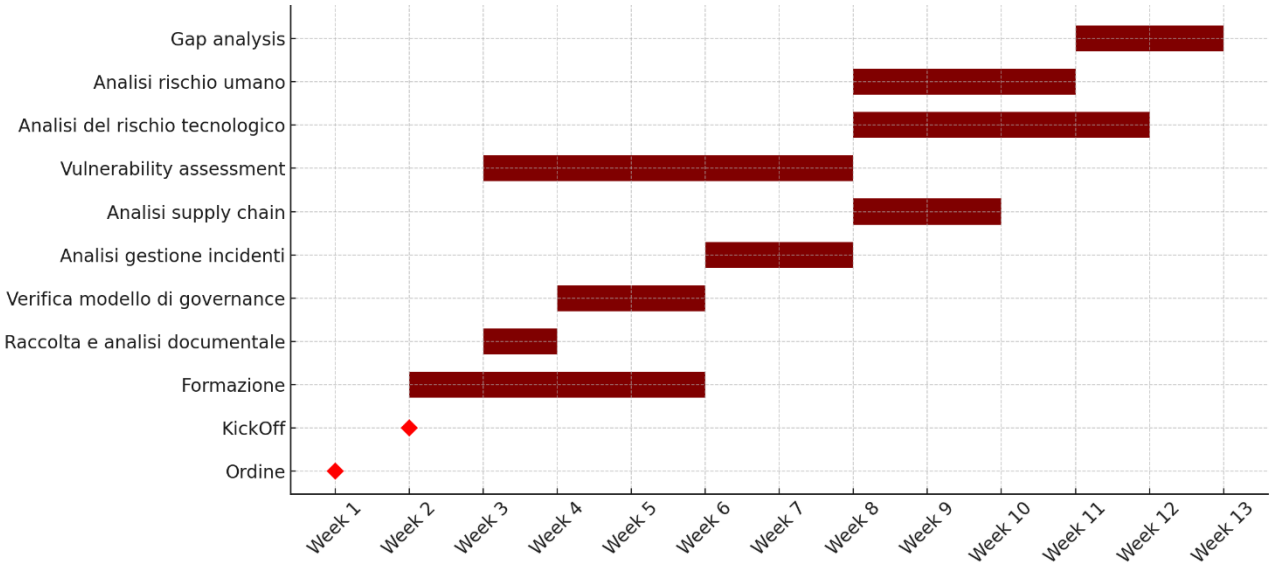
Gestione della postura di sicurezza e visibilità di rete: Supporto per la gestione della postura di sicurezza degli endpoint (Endpoint Security Posture Management), con valutazione delle vulnerabilità, rilevamento delle configurazioni errate e raccomandazioni di remediation. Parallelamente, la componente di Network Detection and Response (NDR) offre visibilità approfondita sul traffico di rete, consentendo l'identificazione di comportamenti sospetti come esfiltrazioni di dati, beaconing o movimenti laterali, grazie alla correlazione di eventi tra rete, endpoint e identità.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

8 PIANO DI LAVORO

8.1 GANTT

In fase di avvio del progetto verrà concordato un cronoprogramma operativo delle attività progettuali, con identificazione dei referenti, delle milestone e dei rilasci.
Viene di seguito fornito un GANTT esemplificativo che sarà contestualizzato in funzione della data di avvio del progetto, delle disponibilità del Cliente e delle modalità operative concordate.



Si prevede che l'attività verrà svolta prevalentemente da remoto, tramite piattaforma di videoconferenza MS Teams o piattaforme analoghe messe a disposizione dal Cliente.

8.2 PIANO DI PRESA IN CARICO

Di seguito si riportano le principali attività:

- predisposizione e configurazione dei servizi proposti;
- creazione dell'account del referente dell'Amministrazione per l'accesso al Portale della Fornitura e configurazione dell'Area Privata;
- acquisizione di know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione;
- acquisizione degli standard, modalità operative, linee guida e metodologie in uso presso l'Amministrazione, ove presenti.

Entro 30 giorni dalla stipula del Contratto esecutivo verrà svolta la prima riunione di lavoro con il referente tecnico del Fornitore ed i referenti tecnici dell'Amministrazione.
A seguito di tale riunione la presa in carico prevederà:

- Identificare il team di progetto;

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- verrà designato un team di progetto che lavorerà sulla presa in carico del servizio IT e verrà definito un responsabile del progetto.

Definizione del piano di attuazione:

- sarà creato un piano di attuazione che includa un calendario per l'implementazione del servizio IT e delle attività di acquisizione di conoscenze, standard e linee guida.
- Acquisizione di informazioni sull'organizzazione: verranno raccolte le informazioni sul contesto organizzativo, tecnologico e funzionale dell'Amministrazione attraverso la revisione della documentazione disponibile, interviste con i rappresentanti dell'Amministrazione, e visite sul campo.

Acquisizione di standard e metodologie:

- Rivedere gli standard, le modalità operative, le linee guida e le metodologie in uso presso l'Amministrazione per integrare le migliori pratiche in uso e conformarsi ai requisiti dell'Amministrazione.

Formazione del personale:

- il personale coinvolto nella presa in carico del servizio sarà formato “on the job” in modo da assicurare la conoscenza dei processi dell'organizzazione e dei protocolli standard.

Test del servizio:

- il servizio sarà testato con i rappresentanti dell'Amministrazione per valutare l'efficacia dell'implementazione e identificare eventuali problemi o aree di miglioramento.

Conduzione del servizio IT:

- la conduzione del servizio avverrà effettuando monitoraggi sulle performance per valutare l'efficacia dell'implementazione, identificando eventuali aree di miglioramento.

Rapporti periodici:

- verranno forniti report periodici all'Amministrazione sulle prestazioni del servizio, sull'avanzamento delle attività e linee guida per garantire una comunicazione continua e trasparente

L'attività di presa in carico dovrà essere completata entro il termine massimo di un mese solare dalla data di stipula del Contratto esecutivo. In caso contrario, l'Amministrazione si riserva il diritto di richiedere l'applicazione della relativa penale prevista nel contratto.
Durante l’attività di Presa in carico si garantirà:

- la presenza di tutte le figure coinvolte per l’erogazione dei servizi nonché dovranno essere reperibili e disponibili i Referenti Tecnici;
- la predisposizione di un verbale attestante il completamento della presa in carico da redigere secondo le indicazioni fornite dall’Amministrazione e che dovrà essere sottoscritto dal RTI e dall’Amministrazione.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

8.3 SPECIFICHE DI COLLAUDO

La progettazione e l'implementazione di un servizio MDR Standard e MDR Advanced prevede l'esecuzione delle attività di seguito descritte, secondo il seguente flusso operativo.

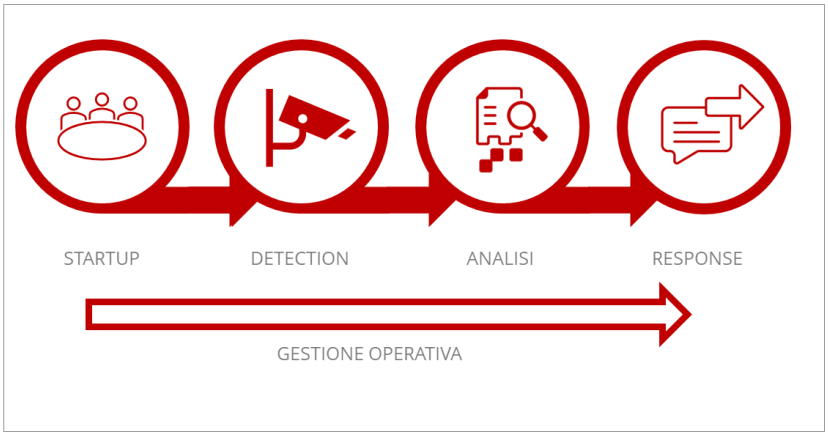


Figura 5 – Servizio Security Monitoring & Respon: flusso operativo

Preparazione

La fase *Preparazione* è essenziale nella progettazione e implementazione di un servizio di Security Monitoring & Response. Durante questa fase, si gettano le basi operative, tecnologiche e organizzative del servizio. La fase di preparazione si articola secondo le seguenti fasi:

Kickoff: sessione introduttiva con il Cliente per illustrare il processo di onboarding e presentare una panoramica della soluzione EDR Cynet. Durante la conferenza vengono delineati i dettagli del servizio, comprese le modalità di interazione con gli analisti SOC, la gestione dei report di sicurezza e l'utilizzo del portale Cynet MDR.

Onboarding: è la fase iniziale in cui Maticmind e il Cliente collaborano per configurare e integrare il servizio MDR nell'infrastruttura IT del cliente, con l'obiettivo di garantire che il servizio sia completamente operativo, personalizzato in base alle esigenze del Cliente e pronto per monitorare, rilevare e rispondere alle minacce di sicurezza. Le attività tipicamente erogate in questa fase possono essere sintetizzate come segue:

- Attivazione dell'account Cynet del Cliente per il Servizio EDR.
- Creazione e profilazione degli Utenti del Cliente e del Cyber Defence Center per l'accesso al management della soluzione EDR Cynet.
- Creazione dei gruppi di utenti utilizzatori della soluzione
- Condivisione con il Cliente dei package per l'installazione degli agent sugli EndPoint;
- Supporto al Cliente per la distribuzione e installazione degli Agent.

Documentazione: questa fase prevede la definizione della documentazione necessaria nella conduzione del servizio di MDR. Questa potrà includere, a titolo esemplificativo ma non esaustivo:

- Procedure e processi operativi per il monitoraggio degli eventi di sicurezza, per la segnalazione e per l'escalation verso il Cliente di allarmi e incidenti di sicurezza.
- Playbook condivisi per la gestione degli allarmi e degli incidenti di sicurezza.

Tuning: questa fase prevede il monitoraggio iniziale per analizzare i dati raccolti e identificare

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

eventuali falsi positivi, seguito dalla regolazione delle policy di rilevamento per adattarle all'ambiente operativo del cliente, minimizzando i falsi allarmi. Viene inoltre effettuata la personalizzazione degli alert, configurando notifiche su misura per i responsabili della sicurezza in base ai livelli di criticità.

Composizione Team

Il Team, responsabile dell'esecuzione delle attività del servizio Security Monitoring & Response è composto da figure altamente qualificate ed esperte nel campo della cybersecurity.
Queste strutture forniscono supporto al Team, contribuendo all'erogazione di un servizio ad alto valore aggiunto, garantendo altresì qualità e conformità dei servizi erogati a regolamenti e best practices applicabili. Il Team è strutturato in due macro-unità: Team di Governo e Team Operativo.

Team di governo

Il Team di Governo è composto dal Service Manager, a cui è assegnata la responsabilità del coordinamento di tutte le attività e di interfaccia nei confronti del Cliente. In particolare, il Service Manager ha il compito di gestire, pianificare, coordinare e monitorare lo svolgimento di tutte le attività richieste.

Team Operativo

Il Team Operativo è incaricato dell'esecuzione delle diverse attività e dei servizi inclusi nel servizio Security Monitoring & Response. Il Team Operativo è organizzato in due livelli:

- ✓ Team di analisti di sicurezza
- ✓ Team specialistico di analisti di sicurezza

9. TABELLA RIEPILOGATIVA DEI SERVIZI E RELATIVI IMPORTI CONTRATTUALI

di seguito si riporta allegato 4

Allegato%204%20-%
20Preventivo%20Ecor

ALLEGATO 4 PREVENTIVO ECONOMICO

Gruppo TIM - Uso Interno - Tutti i diritti riservati.