REGIONE DEL VENETO

**PROCEDURA APERTA TELEMATICA, AI SENSI DELL'ART. 71 DEL D.LGS. N. 36/2023 E SS.MM.II, PER L'ACQUISTO DI SERVIZI DI SICUREZZA PER IL CSIRT REGIONALE DELLA DURATA DI 48 MESI, IN DUE LOTTI.**

CODICE GARA APPTEL: **G03944**

Lotto 1 CUI: **S80007580279202600043**

Lotto 2 CUI:

**S80007580279202600044** - **S80007580279202400040** - **S80007580279202400043** - **S80007580279202500049**

# CAPITOLATO TECNICO

**Indice**

# CAPITOLATO TECNICO DI GARA

## Art. 1 - Condizioni generali

### 1.1 Premessa

Il presente Capitolato Tecnico ha per oggetto la conduzione operativa, l'evoluzione ed il miglioramento continuo di un serie di servizi integrati di cybersecurity a supporto degli Enti facenti parte dello CSIRT della Regione del Veneto (DGR n. 1024 del 222.8.2023). Per un maggior dettaglio dell'attuale contesto del Csirt regionale si rimanda all'allegato C2.

I servizi dovranno essere forniti con una logica "**chiavi in mano**" ed "**End-to-End**" (E2E). Questo implica una gestione unitaria e coordinata di persone, processi e piattaforme a supporto. Gli Aggiudicatari si assumono la piena responsabilità di accompagnare i destinatari del servizio, dalla fase iniziale di identificazione della necessità/criticità fino alla loro completa risoluzione e alla produzione della relativa documentazione (evidenze).

L'erogazione delle prestazioni da parte del fornitore dovrà avvenire nel pieno rispetto del quadro normativo e dell'assetto organizzativo propri dell'Ente beneficiario, adattandosi alle sue peculiari caratteristiche tecnologiche e dimensionali. Considerato il valore strategico e l'articolazione tecnica delle attività previste, nell'espletamento dei servizi sono richiesti massimi livelli di tempestività, proattività, rigore metodologico e tutela della riservatezza.

Il modello operativo del CSIRT Regionale è di tipo **"Campus"** che adotta un approccio ibrido e federato, progettato per gestire un ecosistema eterogeneo di pubbliche amministrazioni, enti strumentali, sanità e società partecipate (la *Constituency*).

In questo modello, **il CSIRT eroga centralmente i servizi e definisce linee guida standardizzate, ma ogni singolo Ente mantiene la responsabilità operativa sul proprio perimetro**. L'obiettivo è creare una comunità (il "campus") in cui si condividono risorse e informazioni, come ad esempio gli Indicatori di Compromissione (IoC) generati dai SOC locali degli Enti più maturi, a beneficio di tutta la rete

Il funzionamento del modello Campus si basa su principi di integrazione e sussidiarietà:

- **Standardizzazione e Linee Guida centralizzate**: il CSIRT centrale fornisce la bussola metodologica (tassonomie, template, procedure e metriche KPI/KRI comuni) affinché tutti gli Enti parlino la stessa lingua.
- **Responsabilità Operativa distribuita**: sebbene il monitoraggio e l'indirizzo siano centralizzati, l'attuazione materiale delle bonifiche (es. patch di sistemi, isolamento fisico di una macchina) rimane in capo ai team IT del singolo Ente.
- **Condivisione delle Risorse (Information Sharing)**: gli Enti con un livello di maturità più elevato (es. quelli dotati di un proprio SOC locale) condividono le proprie risorse e le proprie telemetrie con il nodo centrale, che a sua volta le redistribuisce per proteggere gli altri Enti della Constituency.

Per far funzionare il modello Campus, la governance è strutturata su livelli gerarchici ben definiti:

- **Livello Strategico (Comitato Strategico)**: È l'organo direttivo supremo presieduto dalla Regione e partecipato dai referenti degli Enti principali e dalle autorità nazionali (es. ACN, Polizia Postale). Definisce il piano pluriennale, approva il modello di adesione e funge da punto di escalation per incidenti gravissimi.
- **Livello Direttivo (Comitato Direttivo)**: È guidato dal Responsabile del CSIRT e dai CISO/CIO degli Enti aderenti. Traduce la strategia in processi operativi, valuta le minacce in corso e indirizza l'erogazione dei servizi.
- **Livello Operativo Locale (Referenti di Sicurezza degli Enti)**: Ogni Ente del "campus" deve nominare un referente che funge da interfaccia unica verso il CSIRT centrale. Questo referente ha il compito di garantire la corretta erogazione dei servizi, recepire le linee guida e coordinare le attività tecniche all'interno del proprio Ente.

Per governare questo ecosistema, la struttura centrale del CSIRT è divisa in 3 team specializzati: il **Team Governance** (per l'amministrazione, i rapporti con i fornitori e il monitoraggio del budget), il **Team Security Strategy** (per le attività consulenziali su gestione del rischio, business continuity e formazione) e il **Team Esperti Cyber** (per il monitoraggio operativo di minacce, vulnerabilità e incidenti).

## 1.2 Oggetto della fornitura e contesto di applicazione

I servizi di cybersecurity oggetto del presente Capitolato Tecnico sono destinati agli Enti facenti parte della *Constituency* del CSIRT Regionale. Si tratta di un ecosistema eterogeneo che raggruppa le pubbliche amministrazioni regionali, suddiviso in 5 Gruppi con livelli di rischio differenziati. Fanno parte del perimetro le Strutture Sanitarie e Sociali (coordinate da Azienda Zero), gli Enti pubblici regionali strumentali, le Società a partecipazione regionale maggioritaria e il Consiglio Veneto e ulteriori enti autorizzati nel corso degli anni dal Comitato Strategico (per il dettaglio completo si rimanda all'APPENDICE A).

Nella tabella seguente è riportato l'elenco dei servizi oggetto di fornitura, suddivisi per Lotto:

| Lotto | ID Servizio | Servizio |
|---|---|---|
| Lotto 1 | *L1.1* | Governance, controllo e supporto normativo |
| | *L1.2* | Servizio di Reperibilità in caso di Crisi |
| Lotto 2 | *L 2.1* | SOC, Incident Management e Cyber Threat Intelligence |
| | *L2.2* | Vulnerability Management |
| | *L2.3* | Gestione del Rischio, TPRM e Business Continuity |

| | | |
|---|---|---|
| | *L2.4* | Formazione e Security awareness |

Gli Aggiudicatari di ciascun Lotto sono tenuti a presentare un'offerta che distingua chiaramente i costi per tutti i servizi previsti nella suindicata tabella a copertura dell'intera *Constituency*, con una ripartizione per Gruppo di appartenenza (vedi Appendice A).

Tale strutturazione dei costi è essenziale per agevolare la Stazione Appaltante nell'identificazione della spesa relativa ad ulteriori Enti che dovessero essere inclusi nella *Constituency* in un momento successivo all'aggiudicazione dell'appalto.

## 1.3 Acronimi

| Acronimo | Forma estesa | Descrizione sintetica |
|---|---|---|
| ACN | Agenzia per la Cybersicurezza Nazionale | Autorità nazionale di riferimento per la sicurezza cibernetica (D.L. n. 82/2021) |
| AI | Artificial Intelligence — Intelligenza Artificiale | Sistemi tecnologici atti all'automazione di analisi e decisioni tramite simulazione cognitiva |
| ATT&CK | Adversarial Tactics, Techniques and Common Knowledge | Base di conoscenza MITRE per la mappatura di tattiche e tecniche offensive |
| CACAO | Collaborative Automated Course of Action Operations | Standard OASIS per l'interoperabilità e la condivisione di playbook di risposta |
| CMDB | Configuration Management Database | Repository centralizzato degli asset e delle configurazioni dei sistemi ICT |
| CRA | Cyber Resilience Act | Regolamento (UE) 2024/2847 relativo ai requisiti di sicurezza per i prodotti digitali |
| CSIRT | Computer Security Incident Response Team | Nucleo tecnico per la gestione e risposta agli incidenti; a livello nazionale afferisce ad ACN |
| CTI | Cyber Threat Intelligence | Attività di analisi e contestualizzazione informativa sulle minacce cibernetiche |

| | | |
|---|---|---|
| CVE | Common Vulnerabilities and Exposures | Nomenclatura standard per l'identificazione univoca delle vulnerabilità informatiche note |
| CVSS | Common Vulnerability Scoring System | Metrica standard per la classificazione della gravità delle vulnerabilità (scala 0-10) |
| DICOM | Digital Imaging and Communications in Medicine | Standard per il trattamento e lo scambio di immagini radiologiche e informazioni correlate |
| ECS | Elastic Common Schema | Specifiche per la normalizzazione dei log, sviluppate da Elastic |
| ENISA | European Union Agency for Cybersecurity | Agenzia dell'Unione Europea incaricata di garantire un elevato livello di cybersicurezza |
| FHIR | Fast Healthcare Interoperability Resources | Protocollo per l'interscambio rapido di dati clinici e sanitari |
| GDPR | General Data Protection Regulation | Regolamento (UE) 2016/679 in materia di protezione e libera circolazione dei dati personali |
| HL7 | Health Level Seven | Standard internazionali per il trasferimento di dati clinici e amministrativi tra software sanitari |
| HTTP | HyperText Transfer Protocol | Protocollo di rete per la trasmissione di ipertesti e risorse sul World Wide Web |
| ICS | Industrial Control Systems | Sistemi di controllo industriale; riferimento per il framework MITRE specifico per domini OT |
| IoC | Indicator of Compromise — Indicatore di Compromissione | Evidenza tecnica rilevata su reti o sistemi indicativa di una avvenuta o tentata violazione di sicurezza |
| IoMT | Internet of Medical Things | Rete di dispositivi medicali connessi (pompe, monitor, diagnostica) per scopi clinici |
| ISAC | Information Sharing and Analysis Center | Centri per la condivisione collaborativa di informazioni sulle minacce informatiche entro specifici settori |

| | | |
|---|---|---|
| MFA | Multi-Factor Authentication — Autenticazione a più fattori | Procedura di verifica dell'identità basata su due o più fattori di autenticazione indipendenti |
| MISP | Malware Information Sharing Platform | Piattaforma open source per la gestione e la correlazione di indicatori di compromissione e dati di intelligence |
| MITRE | MITRE Corporation | Organizzazione USA no-profit curatrice di framework globali per la sicurezza (ATT&CK e D3FEND) |
| ML | Machine Learning — Apprendimento automatico | Tecnica di IA basata su algoritmi capaci di apprendere pattern dai dati in modo non esplicitamente programmato |
| MTTD | Mean Time to Detect | Tempo medio intercorrente tra la genesi di un incidente e il suo rilevamento operativo (SOC) |
| MTTR | Mean Time to Respond | Tempo medio necessario per completare le fasi di risposta e contenimento post-rilevamento |
| MxDR | Managed Extended Detection and Response | Servizi di monitoraggio e risposta integrata su endpoint, rete, cloud e infrastrutture d'identità |
| NDR | Network Detection and Response | Tecnologie di analisi del traffico di rete per l'identificazione di minacce senza agent sugli endpoint |
| NIS2 | Network and Information Security Directive 2 | Direttiva (UE) 2022/2555 sulla sicurezza di reti e sistemi, recepita dal D.Lgs. 138/2024 |
| NVD | National Vulnerability Database | Database NIST degli USA per la catalogazione standardizzata e il monitoraggio delle CVE |
| OCSF | Open Cybersecurity Schema Framework | Schema aperto atto all'interoperabilità e normalizzazione di eventi tra diverse piattaforme di sicurezza |

| | | |
|---|---|---|
| OEPV | Offerta Economicamente più Vantaggiosa | Metodo di aggiudicazione (D.Lgs. 36/2023) che pondera profili qualitativi e quantitativi (prezzo) |
| OT | Operational Technology | Sistemi hardware e software dedicati al controllo e al monitoraggio di processi e impianti fisici |
| PACS | Picture Archiving and Communication System | Infrastruttura per la conservazione e gestione centralizzata di immagini cliniche diagnostiche |
| PA | Pubblica Amministrazione | Insieme di organi, enti e istituzioni deputati all'esercizio di funzioni pubbliche |
| PSR | Polo Strategico Regionale | Hub cloud regionale atto all'erogazione di servizi digitali agli enti del territorio veneto |
| REST | Representational State Transfer | Stile architetturale basato su protocollo HTTP per l'interoperabilità tra API web |
| RIS | Radiology Information System | Sistema informatico per la gestione dei flussi di lavoro in reparti radiologici |
| RUP | Responsabile Unico del Procedimento | Garante dell'unità e del corretto svolgimento delle fasi di affidamento ed esecuzione |
| SBOM | Software Bill of Materials | Elenco strutturato dei componenti software, librerie e dipendenze attive in un sistema |
| SIGMA | — | Formato standard per logiche di detection, indipendente dalla specifica piattaforma SIEM |
| SIEM | Security Information and Event Management | Sistema centralizzato per la raccolta, aggregazione e correlazione di log di sicurezza |
| SLA | Service Level Agreement | Patti contrattuali definenti i livelli qualitativi minimi, i tempi di reazione e i regimi sanzionatori |

| | | |
|---|---|---|
| SOC | Security Operations Center | Presidio operativo incaricato del monitoraggio perenne e della risposta a incidenti cyber |
| SOAR | Security Orchestration, Automation and Response | Piattaforma atta all'orchestrazione e automazione dei workflow di risposta agli incidenti |
| STIX | Structured Threat Information eXpression | Standard OASIS per lo scambio di informazioni strutturate sulla Threat Intelligence |
| TAXII | Trusted Automated eXchange of Intelligence Information | Protocollo OASIS per il trasporto sicuro e automatizzato di dati in formato STIX |
| TLP | Traffic Light Protocol | Protocollo cromatico per la gestione dei livelli di riservatezza nella condivisione di intelligence |
| UEBA | User and Entity Behavior Analytics | Analisi comportamentale per il rilevamento di anomalie rispetto a baseline di utenti e asset |
| YARA-L | YARA-Language | Linguaggio di detection nativo per piattaforme Google SecOps/Chronicle |

### 1.4. Durata del contratto

Il Contratto spiega i suoi effetti dalla data della sua sottoscrizione, ovvero dalla diversa data indicata in sede di sottoscrizione del Contratto tra le parti ed avrà termine allo spirare di **48 mesi** decorrenti dalla data di inizio del Contratto.

Pertanto, dalla data di sottoscrizione del Contratto, sarà previsto quanto segue:

● **Periodo di subentro/presa in carico**, non retribuito, della durata di **3 mesi**, dalla data di sottoscrizione del Contratto.

● **Erogazione dei servizi** per una durata complessiva di **45 mesi** dalla data di avvio delle attività, comunicata a mezzo PEC dall'Amministrazione Contraente al Fornitore a conclusione del periodo di subentro.

● **Invio del Piano di Trasferimento del Know how** entro **6 mesi** dalla scadenza del contratto, che dovrà essere approvato dall'Amministrazione regionale.

● **Trasferimento del know-how** entro la fine della fornitura: il Fornitore deve garantire un supporto alla transizione per almeno **3 mesi** prima del termine dell'erogazione dei servizi,

collaborando al trasferimento delle competenze verso l'Amministrazione o un nuovo Fornitore, secondo quanto previsto al paragrafo "*1.10.1 Attività di subentro ed acquisizione Know-How"*.

## 1.5 Modalita' di esecuzione dei servizi

In base alla modalità di esecuzione dei servizi le prestazioni contrattuali dovranno essere svolte come di seguito indicato:

- per i **servizi on-site:** presso le sedi della Stazione Appaltante o presso le sedi degli Enti facenti parte della costituency a cui i servizi sono rivolti;
- per i **servizi erogati da remoto**: presso i Centri Servizi del Fornitore.

Per l'erogazione dei servizi in modalità on-site, la Stazione Appaltante, specificherà le sedi fisiche dove questi ultimi dovranno essere effettuati. In tal caso sono a carico del Fornitore tutti gli oneri e rischi relativi ad eventuali spese di trasporto, di viaggio, di trasferta e di missione per il personale addetto all'esecuzione delle prestazioni, nonché i connessi oneri assicurativi.

Per l'erogazione dei servizi da remoto, gli Aggiudicatari dovranno disporre di strumenti adeguati per la collaborazione con la Stazione Appaltante e gli Enti destinatari dei servizi e per la condivisione della attività al fine di garantire, la partecipazione effettiva e trasparente in modo semplice ed immediato e senza costi aggiuntivi.

### 1.5.1 Orario di svolgimento dei servizi

Tutti i servizi previsti nel presente Capitolato Tecnico, ad eccezione dei servizi "*L1.1 - Servizio di Reperibilità in caso di Crisi*" e "*L2 - SOC, Incident Management e CTI*" dettagliati nei loro rispettivi paragrafi, dovranno essere assicurati con continuità, **dal lunedì al venerdì, dalle ore 9:00 alle ore 18:00**, per tutti i giorni lavorativi dell'anno, senza interruzioni o periodi di chiusura, inclusa la copertura durante i periodi di ferie.

### 1.5.2 Presenza costante e coordinamento dei Lotti

Al fine di assicurare un coordinamento efficiente e reattivo dei servizi oggetto dell'appalto e garantire un'organizzazione ottimale delle attività, è stabilita una rigorosa disciplina in merito alla presenza delle risorse presso la sede della Stazione Appaltante.

Per il Lotto 1, l'Aggiudicatario è tenuto a garantire la presenza fisica costante e ininterrotta presso la sede della Stazione Appaltante di un contingente minimo di **due Full-Time Equivalent (FTE) con profilo senior**. Questa disposizione è fondamentale per assicurare una rapida risoluzione delle problematiche e una perfetta sincronizzazione con le strutture interne della Stazione Appaltante.

Per il Lotto 2, l'Aggiudicatario è tenuto altresì a garantire la presenza fisica costante e ininterrotta presso la sede della Stazione Appaltante di almeno **due Full-Time Equivalent (FTE) con profilo senior**. Questa prescrizione mira a facilitare i processi di *knowledge transfer*, la partecipazione a *daily meeting* e la rapida integrazione con i team interni.

I profili Senior di cui al presente paragrafo rappresentano l'ossatura operativa dell'appalto presso la sede della Stazione Appaltante. Pertanto, tali risorse devono possedere, oltre ai requisiti di seniority qui stabiliti, elevate capacità tecniche, la padronanza documentale e i requisiti di flessibilità e aggiornamento definiti al paragrafo **1.8.1 (Risorse impiegate)**. L'Aggiudicatario è tenuto a garantire che le risorse fisicamente presenti soddisfino pienamente gli standard di eccellenza ivi richiamati, assicurando la necessaria continuità operativa anche in caso di sostituzioni, secondo le modalità previste dal medesimo paragrafo.

### 1.5.3 Modalità di lavoro ibrida per le risorse aggiuntive

Per le ulteriori risorse (FTE aggiuntivi oltre i Responsabili del servizio di ciascun lotto) impiegate nell'esecuzione dei servizi per entrambi i Lotti, l'Aggiudicatario potrà adottare una modalità di lavoro ibrida.

Questa flessibilità permette l'alternanza dell'attività lavorativa tra la modalità **da remoto** e la modalità **in presenza** presso la sede della Stazione Appaltante o degli Enti a seconda del servizio. Tuttavia, per preservare l'efficacia del team e l'integrazione operativa, è stabilito che la modalità **in presenza dovrà avere una prevalenza** rispetto a quella da remoto, sulla base delle disponibilità messe a disposizione della Stazione Appaltante o dagli altri Enti.
In particolare, dovrà essere riportato nella documentazione di rendicontazione periodica, la presenza fisica o remota di ciascuna risorsa.

## 1.6 Principi guida

I principi guida alla base del progetto per il CSIRT Regionale, orientati a garantire scalabilità, misurabilità e una concreta evoluzione verso la resilienza operativa ("Baseline 2.0"), si articolano nei seguenti punti fondamentali:

- **Standardizzazione**: è richiesta l'adozione sistematica di tassonomie, procedure, template operativi e metriche comuni (come KPI e KRI) applicabili a tutti gli Enti aderenti alla Constituency. Questo principio assicura la totale uniformità nella fornitura del servizio e rende i risultati chiari, comparabili e sempre auditabili tra le diverse realtà.
- **Industrializzazione ed efficienza**: al fine di ridurre l'onere operativo sugli Enti, il modello prevede l'adozione di connettori, automazioni e di uno specifico "Onboarding Kit". L'industrializzazione del servizio è essenziale per accelerare i processi di attivazione iniziale (onboarding) e permettere una messa a regime rapida ed efficace per una platea così eterogenea.
- **Approccio continuativo**: si evolve la logica della conformità documentale o delle attività episodiche. La gestione del rischio, delle vulnerabilità e della reale esposizione agli attacchi deve essere intesa come un processo continuo, alimentato dinamicamente dai segnali operativi reali provenienti dal monitoraggio, dagli incidenti e dalla gestione dei cambiamenti (risk-by-signal).
- **Integrazione continua (End-to-End)**: i vari servizi del catalogo non devono operare per compartimenti stagni. I flussi informativi derivanti dalla Cyber Threat Intelligence (CTI), dal SOC, dal Vulnerability Management, dalla Business Continuity e perfino

dalla Formazione devono essere strettamente correlati, alimentandosi in modo reciproco per determinare rapidamente le priorità di intervento e guidare le decisioni operative.

- **Adozione di logiche di automazione controllata (Guardrail)**: l'iniziativa contempla l'implementazione di soluzioni SOAR atte all'orchestrazione dei flussi di risposta mediante appositi *playbook*. L'automazione non deve configurarsi come un processo privo di supervisione, bensì agire entro un sistema di vincoli e iter autorizzativi inderogabili ("guardrail"). Tale fondamento risulta prioritario per le Strutture Sanitarie (domini *safety-critical*), ove è imperativo scongiurare che gli interventi automatici di contenimento interferiscano con la continuità delle cure o la tutela della salute del paziente.

## 1.7 Organizzazione e requisiti delle risorse

Secondo gli standard nazionali e internazionali recepiti da ACN, un CSIRT per poter adempiere al proprio mandato deve essere composto da personale altamente qualificato, con ruoli e responsabilità ben definiti.

### 1.7.1 Risorse impiegate

Considerata la natura strategica dei servizi, le risorse impiegate nell'erogazione degli stessi, dovranno possedere elevate capacità tecniche in ambito sicurezza informatica e professionali quali prontezza, precisione, affidabilità, competenza e perfetta conoscenza della documentazione contrattuale. Tali requisiti di eccellenza tecnica e professionale trovano la loro massima applicazione operativa nel presidio richiesto al paragrafo **1.5.2 (Presenza costante e coordinamento dei Lotti)**. Le risorse destinate a tale presidio fisico devono essere selezionate garantendo la perfetta aderenza a detti standard, alla conoscenza degli strumenti in uso presso l'Amministrazione (vedi par. 2.2) e fungere da figure di interfaccia diretta con la Stazione Appaltante e responsabili del raccordo tra la Governance centrale e le attività operative del CSIRT."

Gli Aggiudicatari dovranno garantire un elevato grado di flessibilità nel rendere disponibili le proprie risorse, nonché nel garantire l'aggiornamento tecnico delle necessarie competenze.

Le nuove risorse professionali che subentrano eventualmente in sostituzione devono possedere certificazioni ed esperienze, per tipologia e durata, non inferiori a quelle della risorsa sostituita.

Si precisa inoltre che eventuali titoli e certificazioni richiesti/offerti in fase di gara, dovranno essere posseduti per l'intera durata contrattuale.

### 1.7.2 Responsabili del servizio

Al fine di garantire la massima efficacia operativa, la continuità dei servizi e un allineamento costante con le esigenze della Stazione Appaltante, l'Aggiudicatario dovrà obbligatoriamente individuare e formalizzare la nomina di un **Responsabile** per ogni servizio del lotto di

riferimento (due Responsabili per i servizi di cui al Lotto 1 e 4 Responsabili per i servizi di cui al lotto 2).

Costui non è una figura meramente formale, ma rappresenta il punto di contatto unico e primario tra gli Aggiudicatari, la Stazione Appaltante e gli Enti. Le sue principali responsabilità includono:

- **interfaccia operativa:** assicurare un canale di comunicazione diretto, efficiente e proattivo con la Stazione Appaltante e, specificamente, con i referenti designati per l'esecuzione dei servizi.

- **gestione tecnica:** essere il responsabile della direzione tecnica e dell'esecuzione del servizio di propria competenza. Ciò include la supervisione della qualità dell'erogazione, il rispetto degli standard contrattuali e il coordinamento delle risorse impiegate.

- **risoluzione di problemi:** agire come *escalation point* di primo livello per qualsiasi problematica tecnica complessa, deviazione dagli SLA (Service Level Agreement) o necessità di coordinamento urgente.

- **reporting e monitoraggio:** fornire periodicamente alla Stazione Appaltante report dettagliati sull'andamento dei servizi, sul rispetto delle metriche di performance e sulle eventuali criticità riscontrate, proponendo soluzioni e piani di mitigazione.

- **evoluzione e adeguamento:** partecipare attivamente ai tavoli tecnici con la Stazione Appaltante per discutere e pianificare gli eventuali aggiornamenti, le evoluzioni tecnologiche o gli adeguamenti normativi necessari ai servizi erogati.

Gli Aggiudicatari dovranno garantire che il Responsabile del servizio designato sia in possesso dei seguenti requisiti:

- **competenza specialistica:** comprovata e approfondita conoscenza tecnica e funzionale dei servizi relativi al lotto di riferimento;
- **reperibilità e tempestività:** piena disponibilità a interfacciarsi con la Stazione Appaltante per ogni necessità di coordinamento;
- **poteri decisionali:** adeguata autonomia all'interno della struttura del Fornitore, tale da garantire decisioni rapide e vincolanti in merito all'esecuzione delle attività e all'allocazione delle risorse.

La Stazione Appaltante si riserva la facoltà di richiedere la sostituzione della figura del Responsabile del servizio designato dagli Aggiudicatori, nel caso in cui le prestazioni o la disponibilità di tale figura non siano ritenute idonee al mantenimento di un'efficiente gestione dei servizi.

## 1.8 Vincoli normativi, tecnologici e principio di indipendenza

Gli Aggiudicatari dei Lotti del presente Capitolato Tecnico, dovranno conformarsi ai seguenti vincoli contrattuali trasversali:

- **qualificazione ACN per servizi da remoto e cloud:** considerata l'elevata criticità delle informazioni trattate (es. log di sicurezza, indicatori di compromissione, assetti vulnerabili e potenziali dati afferenti al perimetro sanitario), tutti i servizi erogati da remoto dal Fornitore e le relative infrastrutture tecnologiche (piattaforme SaaS, PaaS, IaaS) utilizzate per l'erogazione dei servizi oggetto del presente Capitolato, dovranno obbligatoriamente possedere e mantenere attiva per l'intera durata dell'appalto la qualificazione di livello minimo **AC1** (o superiore) rilasciata dall'Agenzia per la Cybersicurezza Nazionale (ACN). Tale requisito è da intendersi come vincolo inderogabile per prevenire attacchi alla catena di fornitura (Supply Chain) e garantire l'idoneità al trattamento di dati strategici e critici della Pubblica Amministrazione.

- **certificazioni aziendali e di servizio:** l'Aggiudicatario di ciascun Lotto dovrà possedere una valutazione di conformità del proprio sistema di gestione della qualità alla norma **UNI EN ISO 9001**, idonea, pertinente e proporzionata al seguente oggetto: "servizi di consulenza tecnico-specialistica e/o organizzativa nell'ambito della sicurezza informatica". L'Aggiudicatario di ciascun Lotto dovrà possedere altresì una valutazione di conformità del sistema di gestione alla norma **UNI EN ISO 27001**, idonea, pertinente e proporzionata al seguente ambito di attività: "servizi di consulenza tecnico-specialistica. organizzativa, strategica nell'ambito della sicurezza informatica e/o continuità operativa". Il possesso di tali certificazioni dovrà essere comprovato entro **10 giorni** dalla proposta di aggiudicazione, pena l'esclusione dalla procedura di gara, mediante la fornitura dei relativi certificati e mantenuto per tutta la durata del contratto. In caso di raggruppamenti temporanei d'impresa, consorzi o aggregazioni di imprese il requisito dovrà essere posseduto da ogni impresa che svolgerà, anche parzialmente, l'attività oggetto delle certificazioni.

- **conformità normativa di riferimento:** l'esecuzione dei servizi dovrà essere costantemente allineata alle direttive europee e nazionali di settore in vigore nel periodo di vigenza del presente appalto, con particolare riferimento al **D.Lgs. 138/2024 (recepimento Direttiva NIS2)**, alla **Legge 90/2024** in materia di cybersicurezza per le pubbliche amministrazioni, all'**AI Act**, al **GDPR** e al Cyber Resilience Act (Regolamento UE 2024/2847) e successivi aggiornamenti.

## 1.9 Attività propedeutiche all'erogazione dei servizi

Per garantire la corretta esecuzione delle prestazioni previste dal presente Capitolato Tecnico, i nuovi Fornitori dovranno svolgere una serie di attività preparatorie alla presa in carico del servizio. Tutti gli oneri e le spese necessarie allo svolgimento di tali attività propedeutiche si intendono interamente compresi e remunerati nel corrispettivo complessivo dei servizi; pertanto, non sarà riconosciuto alcun compenso aggiuntivo o rimborso spese.

### 1.9.1 Attività di subentro ed acquisizione Know-How

Al fine di garantire l'efficacia dei servizi sin dall'avvio della fornitura, è previsto un periodo di presa in carico della durata di **3 mesi solari** durante il quale, il Fornitore subentrante dovrà impiegare un numero di risorse idoneo ad assicurare un efficiente passaggio di consegne da parte dei fornitori uscenti.

Tale personale dovrà essere già pienamente formato e addestrato sulle tematiche tecniche, funzionali, organizzative e normative oggetto dell'appalto, nonché sui metodi, sugli standard e sugli strumenti che saranno utilizzati nel corso del contratto.

Durante questo periodo a titolo completamente gratuito, il Fornitore entrante dovrà garantire entro i primi **15 giorni** lavorativi dalla data di sottoscrizione del contratto:

- l'acquisizione e l'analisi della documentazione pregressa relativa ai servizi erogati;
- la redazione e la consegna del **Piano di Subentro** (come meglio dettagliato al capitolo 4.3).

### 1.9.2. Modello di governo e gestione del personale

Il Fornitore di ogni Lotto, è tenuto a predisporre una struttura di Governo dei servizi. I nominativi del **Responsabile Unico delle Attività Contrattuali (RUAC)** e dei **Responsabili dei servizi** dovranno essere comunicati all'Amministrazione entro **5 giorni solari** dalla stipula del Contratto.

Il RUAC, le cui attività sono già comprese nel corrispettivo contrattuale, avrà la responsabilità di:

- pianificare l'impiego delle risorse e l'organizzazione dei team, trasmettendo tempestivamente all'Amministrazione l'elenco aggiornato dei nominativi assegnati a ciascun servizio.
- monitorare e rendicontare l'andamento dei servizi (es. avanzamento attività, obiettivi, qualità, gestione rischi e verbali d'incontro).
- gestire le assenze e le sostituzioni del personale (ferie, malattie, permessi) per garantire la continuità operativa.

Al fine di garantire la dovuta autonomia organizzativa dall'Amministrazione, resta in capo al Fornitore l'onere di pianificare e aggiornare i turni e i piani di presenza necessari a coprire presidi continuativi, reperibilità, extra-orario o picchi di lavoro.

## 1.10 Affiancamento di fine fornitura (passaggio di consegna)

Al fine di garantire la perfetta continuità operativa delle attività del CSIRT Regionale e della relativa *Constituency*, gli Aggiudicatari saranno tenuti a porre in essere una transizione in uscita strutturata, sicura ed esaustiva di tutti i servizi, processi e piattaforme oggetto del presente Capitolato Tecnico.

Il periodo di *handover* avrà una durata di **3 mesi solari** a decorrere dalla scadenza naturale del vincolo contrattuale, ma la Stazione Appaltante si riserva la facoltà di attivare la medesima

procedura, previa comunicazione formale, anche nell'ipotesi di risoluzione anticipata del rapporto.

Nelle more del completamento di tale fase, il Fornitore uscente collaborerà attivamente con l'Amministrazione e con il soggetto subentrante, mantenendo la responsabilità della gestione contrattuale e garantendo il rispetto dei Livelli di Servizio (SLA) vigenti fino all'ultimo giorno.

L'andamento della transizione sarà monitorato tramite incontri di SAL settimanali, cui prenderanno parte i Referenti dei due Fornitori, i rispettivi DEC e, qualora ritenuto necessario, il RUP e gli Assistenti al DEC.

Durante tale fase, il Fornitore uscente dovrà garantire le seguenti attività minime e vincolanti per il trasferimento completo dei servizi:

- **knowledge transfer e processi:** Trasferimento formale e completo del *know-how* operativo, delle metodologie e delle procedure di lavoro (inclusi Runbook, Playbook di risposta agli incidenti, procedure di Crisis Management e piani di BC/DR);
- **rilascio e decommissioning piattaforme:** Supporto tecnico al decommissioning e al trasferimento di proprietà di tutte le piattaforme e le licenze utilizzate per l'erogazione dei servizi (ove applicabile), garantendo l'assenza di situazioni di *vendor lock-in* tecnologico o metodologico;
- **esportazione dati e log:** completa esportazione di tutti i dati storici, gli indicatori di rischio (KPI/KRI), le telemetrie SOC, i log di sicurezza, i report di Vulnerability Management e i registri dei rischi (Risk Register) in formati aperti, standard e leggibili per garantire la piena portabilità a favore del soggetto subentrante;
- **archiviazione della documentazione:** tutta la documentazione di progetto, i report operativi e i verbali di ogni tipo prodotti dai soggetti Aggiudicatari nell'arco della durata dell'appalto, se non già correttamente archiviati all'interno del repository documentale, dovranno essere resi disponibili (anche in formato editabile .docx, .xlsx, ecc.) alla Stazione Appaltante 30 giorni prima dell'inizio del periodo di handover;
- **revoca delle credenziali:** l'Aggiudicatario è tenuto a garantire una gestione rigorosa e controllata delle procedure di revoca delle credenziali, sia operative che remote, assegnate a sé stesso e al proprio personale entro il termine dell'appalto.

Il fornitore uscente dovrà altresì impegnarsi a mantenere in servizio il **personale chiave** a supporto dell'erogazione dei servizi per l'intera durata del periodo di handover, al fine di assicurare la corretta trasmissione della conoscenza critica ai nuovi fornitori. Dovrà inoltre trasmettere all'Amministrazione, il **"Piano di trasferimento del Know-How"** per la sua approvazione (come meglio dettagliato al cap. 4.4 ).

# Art. 2 - LOTTO 1 - Servizi di Governance, controllo e supporto normativo del CSIRT regionale

## 2.1 Oggetto del servizio

Il presente Lotto è specificamente dedicato alla configurazione, all'avvio e alla gestione del **presidio operativo della Governance del CSIRT Regionale e del presidio di reperibilità in caso di crisi** in seguito ad incidenti.

Il presidio costituisce il nucleo strategico e decisionale per la gestione coordinata della sicurezza cibernetica all'interno del CSIRT Regionale e dovrà assicurare la Governance della sicurezza informatica inerente gli aspetti tecnologici, organizzativi e normativi, coerentemente con il framework dei servizi CSIRT e con l'impostazione richiamata da ACN per la realizzazione e il potenziamento di tali strutture.

Assumendo il ruolo esclusivo di controllo dei servizi, supporto e supervisione critica delle attività dell'intera Constituency (Cabina di Regia Strategica), il CSIRT regionale dovrà essere considerato come nodo territoriale di un ecosistema più ampio, capace di raccogliere segnali dal territorio, fornire servizi agli enti aderenti e interagire con le strutture nazionali.

Le principali attività che dovranno essere garantite dall'Aggiudicatario nella gestione dei servizi del CSIRT dovranno includere:

- il raccordo con l'ecosistema nazionale, inclusi CSIRT Italia, HyperSOC e logiche di information sharing;
- la verifica della conformità periodica dell'adesione degli Enti alle normative, alle linee guida e alle *best practice* in materia di sicurezza informatica;
- il monitoraggio normativo e di settore relativamente a normative nazionali (Decreti Legislativi, Leggi, Circolari e Linee guida emanate da ACN, Linee Guida AGID) ed europee (Regolamenti, Direttive) e identificazione tempestiva degli impatti delle nuove disposizioni sulla struttura organizzativa, i processi e i sistemi informativi della Constituency;
- un supporto nel coordinamento ed un'azione di controllo imparziale sulla corretta esecuzione dei servizi del Lotto 2 del presente Capitolato Tecnico;
- un supporto nella validazione di eventuali tool proposti dall'Aggiudicatario del Lotto 2;
- il supporto nella fase di definizione dei processi e delle procedure operative per la gestione degli incidenti, proponendosi come coordinamento delle risposte agli incidenti maggiori che coinvolgono più Enti, garantendo la tempestiva condivisione delle informazioni e il supporto nell'attivazione di playbook ad hoc o dei piani di *disaster recovery* e *business continuity*;
- la produzione di report periodici (almeno semestrali) sullo stato della sicurezza cibernetica della Constituency da sottoporre agli organismi decisionali;
- la corretta archiviazione della documentazione prodotta nello svolgimento di tutti i servizi presenti nei due Lotti nell'apposito Gestore documentale (v. par. "2.2 Modello architetturale");
- il supporto nell'adozione dell'AI all'interno del contesto del CSIRT al fine di rendere i processi cyber più scalabili, predittivi e adattivi, riducendo l'effort operativo sulle attività

ripetitive, aumentando la capacità di identificazione proattiva delle minacce e accelerando i cicli di analisi, decisione e remediation;

- il supporto nell'attivazione o nel potenziamento di CSIRT territoriali, garantendo la piena coerenza con i requisiti minimi individuati dalle Linee Guida ACN;
- l'assistenza nella gestione delle comunicazioni di crisi a seguito di incidenti, rivolta sia all'interno verso la Constituency sia all'esterno nei confronti delle autorità di settore e della collettività;
- l' assistenza per l'accesso a finanziamenti e bandi di settore (nazionali ed europei) in ambito Cyber Security, garantendo il rispetto dei requisiti richiesti per l'ottenimento dei fondi e il supporto alla successiva rendicontazione;
- il supporto alla migrazione verso il PSR (Polo Strategico Regionale) per quegli Enti della Constituency sprovvisti delle necessarie competenze tecnico-amministrative necessarie a gestire autonomamente le attività indispensabili per la fruizione dei servizi messi a disposizione dal CSIRT, massimizzando l'efficacia dei costi e la resilienza operativa;
- aggiornamento dei contenuti del sito web del Csirt regionale.

### 2.1.1 Supporto normativo

Le attività previste in questo lotto non consistono unicamente nell'istituzione del Centro di Controllo, ma includono anche l'erogazione di un **supporto normativo e regolamentare, con pareri a validità legale** finalizzato ad assistere l'intera Constituency sia nell'assolvimento degli obblighi previsti dal presente Capitolato sia nella gestione di ulteriori adempimenti in materia di cybersicurezza.

L'Aggiudicatario dovrà assumere un ruolo proattivo nel supportare gli Enti nel raggiungimento e nel mantenimento della piena compliance normativa di riferimento e delle best practices di settore in ambito di sicurezza informatica e protezione dei dati.

La conformità dovrà essere garantita e dimostrata rispetto ai seguenti principali pilastri normativi e di indirizzo (ove applicabili a ciascun Ente della Constituency):

- **D.Lgs. 138/2024 (Recepimento Direttiva NIS2):**
    - Obbligo fondamentale per gli enti essenziali e gli enti importanti di implementare misure rigorose di gestione del rischio di cybersicurezza.
    - Supporto specifico nella notifica di incidenti, nella redazione del piano di gestione delle crisi e nell'adozione di un sistema di gestione della sicurezza delle informazioni (SGSI) conforme agli standard di riferimento.
- **Legge 90/2024 (Disposizioni urgenti in materia di cybersicurezza per la PA):**
    - Conformità alle indicazioni operative e di governance emanate dal Dipartimento per la Trasformazione Digitale (DTD) e dall'Agenzia per la Cybersicurezza Nazionale (ACN).
    - Supporto agli Enti che rientrano nel perimetro di applicazione della Legge per l'adeguamento delle proprie strutture e procedure.

- **AI Act & Cloud (Regolamento Europeo sull'Intelligenza Artificiale e Cloud):**
    - Verifica della conformità delle soluzioni di Intelligenza Artificiale eventualmente adottate ai requisiti di trasparenza, *robustezza*, non discriminazione e gestione del rischio previsti dall'AI Act.
    - Affiancamento nell'iter di qualificazione ACN per i servizi Cloud (processo di accreditamento e verifica della conformità dei servizi Cloud utilizzati dalla PA, in linea con le strategie nazionali).
- **GDPR (Regolamento Generale sulla Protezione dei Dati - Reg. UE 2016/679) nell'ambito del CSIRT e nel dominio di cybersicurezza:**
    - Supporto costante e qualificato nel fornire pareri in ambito privacy a beneficio del CSIRT e i componenti della constituency (es. aggiornamento e nella manutenzione dei **r**egistri delle attività di trattamento, gestione del ruolo di Responsabile del Trattamento di Sub-responsabile del dato, assistenza nell'ambito di eventi critici o nella gestione di *Data Breach*, supporto nella risposta alle richieste dei soggetti del CSIRT).
- **Cyber Resilient ACT (Regolamento UE 2024/2847):**
    - fornire chiarimenti e interpretazioni pratiche sui requisiti del CRA, specialmente per quanto riguarda gli obblighi specifici per gli acquirenti (gli Enti) di prodotti digitali.
    - sviluppare linee guida e raccomandazioni operative su come gli Enti possono integrare i requisiti di cybersicurezza del CRA nei loro processi di acquisto e gestione dei fornitori.
    - aiutare gli Enti a implementare processi efficaci per la segnalazione e la gestione delle vulnerabilità scoperte nei prodotti CRA-compliant, facilitando il contatto con i fornitori.

Il servizio dovrà garantire inoltre:

- la redazione di **pareri legali** a favore dei soggetti rientranti nel perimetro, sulle tematiche inerenti la corretta applicazione della normativa **Nis 2, Legge 90 e Cyber Resilient Act** (di seguito anche la "Normativa Cyber");
- la redazione di **pareri legali** a favore dei soggetti rientranti nel perimetro, sulla corretta applicazione della normativa in materia di Intelligenza Artificiale (**AI Act e Legge 132/25)** ("Normativa AI") e integrazione di quest'ultima con la Normativa Cyber. Tale attività potrà comprendere la redazione e aggiornamento su base annuale di linee guida in merito alla corretta effettuazione di risk assessment volti ad individuare le obbligazioni a cui sono soggetti gli enti;
- la verifica che le metodologie, i processi e i tool/framework utilizzati per la Gestione del Rischio e la Business Continuity (vedi Lotto 2 cap. 3.3) siano pienamente allineati, coerenti e conformi con i requisiti e le *best practice* definite dall'**Agenzia per la**

**Cybersicurezza Nazionale** (con particolare riferimento alle linee guida per la resilienza cibernetica, alle direttive NIS2 e al Framework Nazionale per la Cyber Sicurezza e la Data Protection) e al **NIST Cybersecurity Framework** (nelle sue funzioni core *Identify, Protect, Detect, Respond, Recover*, focalizzandosi sulla gestione del rischio e sulla continuità operativa;

- la redazione e l'aggiornamento su base annuale di linee guida in merito alla definizione della governance aziendale cyber, alla luce della corretta applicazione delle disposizioni della Normativa;
- la predisposizione delle clausole cyber standard da inserire nelle richieste di offerta, nei bandi di gara, nei contratti, accordi e convenzioni relativi alle forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete del committente;
- la formazione del personale degli Enti sulle tematiche ai punti precedenti.

Per i soggetti rientranti nel perimetro della normativa NIS (vedi "**APPENDICE A – Perimetro della Constituency e Gruppi di Appartenenza"**) il servizio dovrà garantire inoltre:

- la redazione e aggiornamento su base annuale di linee guida in merito alle attività di aggiornamento annuale sul portale di ACN ivi inclusa quindi l'indicazione operativa per la corretta individuazione dei fornitori rilevanti ed effettuazione di risk assessment sui medesimi con indicazione dei presidi di sicurezza adottati e dei requisiti di sicurezza applicabili ai fornitori rilevanti;
- la redazione e l'aggiornamento su base annuale di linee guida per l'attività annuale di categorizzazione dei servizi ai sensi della normativa NIS 2, comprensiva di indicazioni operative per effettuazione delle analisi correlate;
- la formazione relativa ai punti precedenti.

### 2.1.2 Supporto specialistico per la Cyber Resilienza

L'Aggiudicatario dovrà garantire un supporto mirato a rivedere, strutturare e implementare i processi operativi e di gestione degli incidenti informatici degli Enti della Constituency.

L'obiettivo strategico è quello di allineare i processi degli Enti alle più recenti normative cyber e standard di sicurezza stringenti, eliminando i colli di bottiglia operativi e riducendo al minimo i tempi di rilevamento, contenimento e risoluzione degli attacchi informatici.

La revisione e la progettazione dei flussi dovranno essere eseguite tenendo in considerazione i seguenti elementi chiave:

- **standardizzazione della gestione delle crisi cyber:** integrazione di *playbook* standardizzati per la gestione efficace delle crisi di sicurezza informatica.
- **conformità e tempestività nelle notifiche:** adeguamento dei processi per garantire la notifica degli incidenti gravi entro i termini di legge.
- **rafforzamento della resilienza:** potenziamento della resilienza operativa digitale.
- **integrazione immediata dei flussi:** assicurare l'integrazione immediata tra la

procedura di gestione degli incidenti del CSIRT e il processo di notifica delle violazioni dei dati personali al Garante per la Protezione dei Dati Personali.

Il supporto dovrà prevedere le seguenti fasi operative:

- mappatura dei flussi di difesa attuali, identificazione delle vulnerabilità procedurali, dei ritardi nella rilevazione delle minacce (*pain points*) e dei gap di conformità rispetto alle normative cyber;
- disegno dei nuovi processi di *Incident Response*. Definizione chiara di ruoli e responsabilità in caso di crisi (es. **Matrice RACI** per stabilire chi analizza l'allarme, chi isola la minaccia e chi autorizza il ripristino) e integrazione di strumenti di automazione (SOAR/SIEM) ove in uso.
- test dei nuovi processi in ambienti controllati. Esecuzione di **simulazioni di attacco** (es. phishing o ransomware) per verificare la tenuta dei flussi progettati e il coordinamento del team.
- affiancamento nel passaggio alle nuove procedure, addestramento del personale interessato degli Enti, aggiornamento di tutta la documentazione tecnica e operativa interna.

### 2.1.3 Elaborazione di Newsletter e Bollettini di sicurezza:

Il servizio richiesto abbraccia l'intero ciclo di vita della comunicazione informativa, focalizzandosi sull'elaborazione, la redazione e la successiva diffusione di strumenti informativi periodici, ovvero ***newsletter* e *bollettini di sicurezza***.

Queste comunicazioni hanno un duplice scopo:

- **Newsletter:** fornire un aggiornamento periodico e sintetico sulle principali attività svolte, sui progetti in corso, sulle novità normative o procedurali rilevanti e, in generale, sulle informazioni di interesse generale per il pubblico di riferimento (interno o esterno all'Ente, a seconda del target). Periodicità almeno bimestrale.

- **Bollettini di sicurezza:** rappresentare uno strumento di comunicazione urgente e mirato, specificamente focalizzato sull'identificazione, l'analisi e la mitigazione di potenziali vulnerabilità, minacce informatiche (zero-day, malware, attacchi phishing/ransomware) o incidenti di sicurezza verificatisi. Devono contenere istruzioni chiare e actionable (es. patch da applicare, configurazioni da modificare, best practice da seguire) per garantire la protezione dei sistemi informativi e dei dati. Periodicità almeno mensile.

**Gestione delle emergenze e dei bollettini di sicurezza:**

Oltre alla pianificazione standard, è prevista l'emissione di bollettini di sicurezza ad hoc con frequenza immediata, al verificarsi di eventi critici, emergenze o minacce emergenti che richiedano una risposta tempestiva fuori dalla periodicità ordinaria. Tale modalità garantisce un equilibrio ottimale tra continuità informativa e reattività operativa. Al fine di evitare fenomeni di information overload, l'Aggiudicatario dovrà profilare i contenuti in base all'infrastruttura tecnologica dei singoli Enti, veicolando esclusivamente le comunicazioni pertinenti allo specifico parco installato.

L'attività editoriale, estesa a newsletter e bollettini di sicurezza, dovrà articolarsi nelle seguenti fasi:

- **Elaborazione e Analisi:** Ricerca, selezione e contestualizzazione delle informazioni di maggiore rilevanza e attualità.
- **Redazione:** Stesura dei contenuti con stile chiaro, professionale e aderente agli standard editoriali condivisi.
- **Validazione:** Verifica e approvazione interna dei contenuti prima della diffusione.
- **Diffusione:** Invio ai destinatari target tramite i canali di comunicazione ufficiali, assicurando la piena tracciabilità e il monitoraggio dell'avvenuta consegna.

La tempestività nella diffusione delle informazioni, in particolare per i bollettini di sicurezza, dove la rapidità è cruciale per la prevenzione dei rischi dovrà essere rispettata.

### 2.1.4 Valutazione e monitoraggio continuo dei Servizi

L'Aggiudicatario è responsabile di stabilire e mantenere un ciclo continuo di valutazione, implementazione e verifica di tutti i servizi forniti dal CSIRT incluse le misure di sicurezza ad essi correlati.

Le attività principali in carico all'Aggiudicatario comprendono:

- **analisi dei divari (gap analysis) e audit di conformità:** effettuare Gap Analysis dettagliate, confrontando l'infrastruttura, le applicazioni e i processi in uso con i principali standard di sicurezza nazionali (come quelli emanati da AgID e la Direttiva NIS) e internazionali (es. ISO/IEC 27001, NIST). Condurre audit di sicurezza periodici (con frequenza minima semestrale) e verifiche tematiche *ad hoc* volti a valutare la conformità in ambito tecnico, organizzativo e procedurale, coprendo sia la sicurezza logica che quella fisica.
- **verifica e validazione degli interventi eseguiti:** verificare e validare periodicamente l'effettiva efficacia delle attività implementate e misurare le performance di tutti i servizi erogati dal CSIRT.

### 2.1.5 Servizio di Reperibilità in caso di Crisi

L’aggiudicatario dovrà prestare un servizio di reperibilità h24 per 365 giorni all’anno (H24x7x365), al fine di garantire una continuità operativa e una capacità di reazione immediata da parte del CSIRT a fronte di incidenti di sicurezza a elevata criticità avvenuti all’interno della Constituency.

Tale servizio dovrà assicurare la disponibilità costante di personale tecnico specialistico in grado di supportare gli Enti nel contenimento e nella risoluzione di crisi cibernetiche derivanti da incidenti ad impatto critico — quali attacchi ransomware, indisponibilità di servizi essenziali ed esfiltrazione di dati — occorsi agli Enti della Constituency.

Il servizio dovrà altresì assicurare il supporto alla conferma e qualificazione degli eventi segnalati dagli Enti, al fine di determinare l'effettiva natura di "crisi" e valutare la necessità di supporto.

A fronte di tali eventi, l'Aggiudicatario dovrà attivare, se necessario, War Room dedicate e i relativi playbook di risposta. All'interno della War Room, è prevista la partecipazione del Service Manager (quale punto di riferimento contrattuale unico del Servizio del Lotto 2) con la responsabilità di coadiuvare la governance regionale sull'evoluzione della crisi. La reperibilità dovrà coprire senza interruzioni anche i periodi festivi e feriali, garantendo il rispetto dei tempi di reazione e degli SLA inderogabili previsti per gli incidenti di massima severità.

## 2.2 Soluzioni e strumenti a disposizione

L'Aggiudicatario dovrà presentare una proposta per l'erogazione dei servizi robusta, basata su un approccio metodologico che includa in modo sinergico la **configurazione, la parametrizzazione e l'integrazione** di una suite di strumenti tecnologici essenziali per l'efficace funzionamento del CSIRT regionale e la gestione della sua *Constituency*.

Tale approccio dovrà essere improntato sull'utilizzo di soluzioni software già in uso presso la Stazione Appaltante, prevedendo ove necessario l'estensione di ulteriori licenze, feautures o integrazioni con altri software esterni ritenuti necessari per l'esecuzione dei servizi.

Entrando nel dettaglio, l'Aggiudicatario dovrà prevedere l'utilizzo dei seguenti tool già in uso presso l'Amministrazione:

- **Sistema di Ticketing:** un sistema per la gestione strutturata e tracciabile degli incidenti di sicurezza (*Security Incident Response*) e delle richieste di supporto (*Service Request*) da parte degli Enti (Sysaid). Dovrà garantire la categorizzazione degli eventi, l'assegnazione automatica, la definizione di SLA (*Service Level Agreement*), l'escalation automatica e la storicizzazione completa di tutte le attività e le comunicazioni relative a ciascun *ticket*.

- **Tool per la Gestione del rischio:** un sistema collaborativo utilizzato per la gestione del rischio aziendale in conformità dei principali standard e regolamenti (Risk value).

- **Piattaforma di Business Intelligence (BI) e monitoraggio:** piattaforma analitica che consenta il monitoraggio in tempo reale delle metriche operative del CSIRT e la relativa reportistica (*vedi paragrafo 2.3.2 Reportistica*). Tali dati sono cruciali per il *management* e per l'identificazione di aree di miglioramento (Qlik).

- **Sistema di messaggistica crittografato e sicuro:** utilizzo di una Community dedicata alla comunicazione, in grado di garantire la massima riservatezza e integrità delle informazioni scambiate tra i membri del CSIRT e all'interno della *Constituency*. È fondamentale che tale strumento utilizzi protocolli di crittografia *end-to-end* robusti e sia conforme alle normative vigenti in materia di protezione dei dati sensibili e classificati, specialmente in contesti di gestione di crisi (Whatsapp).

- **Repository documentale centralizzato e sicuro:** sistema di gestione documentale che dovrà contenere ad es. policy, procedure, linee guida, analisi di *malware*, i rapporti di *incident response*, verbali dei SAL, ulteriore documentazione tecnica e la reportistica

di ogni servizio prodotti durante tutta la durata dell'appalto. Il repository documentale dovrà garantire un controllo degli accessi granulare, permettendo ai diversi Enti della *Constituency* di accedere esclusivamente ai documenti a loro pertinenti, assicurando al contempo l'immutabilità e la tracciabilità delle versioni dei documenti (Next Cloud).

- **Sistema per la gestione delle credenziali (IAM/IDM):** soluzione per la gestione centralizzata delle identità e degli accessi (*Identity and Access Management - IAM*) degli operatori del CSIRT e, ove necessario, della *Constituency* per l'accesso ai servizi condivisi. Questo sistema è essenziale per implementare politiche di *strong authentication* (es. MFA - *Multi-Factor Authentication*), per la revoca tempestiva degli accessi e per garantire il principio del *least privilege (Dominio AD, Monokee)*.

- **Sistema di posta elettronica:** soluzione che preveda l'utilizzo di una o più caselle di posta elettronica dedicate ai servizi di entrambi i Lotti sulla base delle necessità individuate. Queste caselle saranno configurate con la funzionalità di delega, permettendone così agli Aggiudicatari la gestione operativa. Tutte le caselle di posta elettronica create saranno accessibili alla Stazione Appaltante, al fine di consentire il monitoraggio delle attività e l'andamento dei servizi stessi (Google Gmail).

L'Aggiudicatario avrà la responsabilità di assicurare la **completa integrazione funzionale** tra tutti questi *tool* e altri che potrà proporre in ottica di miglioramento al fine di creare un ecosistema operativo coeso, efficiente e sicuro.

Qualsiasi proposta che implichi la necessità di scrivere codice applicativo *custom* necessario per l'integrazione tra i tool o con altre soluzioni ritenute necessarie, dovrà essere preventivamente approvata dalla Stazione Appaltante.

### 2.2.1 Gestione e mantenimento delle abilitazioni e degli accessi

L'Aggiudicatario è tenuto a garantire una gestione rigorosa e puntuale delle abilitazioni di accesso e dei profili utente relativi ai tool utilizzati, nonché degli accessi delegati alle caselle di posta elettronica, al fine di assicurare la sicurezza, la conformità e l'efficacia operativa.

Con cadenza trimestrale, l'Aggiudicatario dovrà inoltrare alla Stazione Appaltante un **rapporto dettagliato e aggiornato** contenente i seguenti elementi:

- **elenco completo degli utenti abilitati:** una lista esaustiva di tutti gli utenti attualmente abilitati all'utilizzo dei *tool* specificati nel presente capitolato;
- **elenco degli accessi in delega:** una lista di tutti gli utenti autorizzati ad accedere in delega alle caselle di posta elettronica attivate;
- **dettaglio delle modifiche: i**ndicazione dei nominativi (nome, cognome, ruolo/funzione) per i quali sono state concesse abilitazioni/rimozioni/variazioni/deleghe ai *tool* o un nuovo accesso in delega alle caselle di posta elettronica durante il periodo di riferimento.

Viene stabilito che l'onere e la responsabilità della **tempestiva rimozione** delle abilitazioni e/o della **cessazione dell'utente** ricadono esclusivamente sull'Aggiudicatario.

In particolare, per ogni cessazione del rapporto di lavoro, al cambio di funzione o alla necessità di revoca dell'accesso per un determinato utente, l'Aggiudicatario dovrà procedere alla

disabilitazione tempestiva dell'utenza, salvo diverse pattuizioni concordate per particolari esigenze operative.

L'Aggiudicatario è altresì responsabile del monitoraggio delle risorse interne al fine di identificare proattivamente e disattivare gli account degli utenti non più in forza o che non necessitano più di tali accessi, in coerenza con le politiche di *identity management* e *least privilege* definite.

Tale adempimento è considerato essenziale ai fini del mantenimento dei requisiti di sicurezza logica e del corretto utilizzo delle risorse assegnate.

Sarà considerato un elemento migliorativo l'integrazione e successiva possibilità di consultazione di tali informazioni sul **Sistema di Business Intelligence (BI) e Monitoraggio.**

## 2.3 Requisiti minimi e deliverable di governance

L'Aggiudicatario, in qualità di soggetto responsabile della Governance del progetto, è tenuto a garantire una solida struttura di coordinamento e di indirizzo strategico per l'efficace erogazione di tutti i servizi e le attività del CSIRT Regionale. Tale ruolo centrale è fondamentale per assicurare il corretto allineamento con le strategie regionali e per stabilire un raccordo operativo costante e strutturato con l'HUB Sanitario (Azienda Zero), in particolare per le tematiche di sicurezza e formazione che intersecano il dominio sanitario.

Per raggiungere questi obiettivi, l'Aggiudicatario dovrà adempiere, in modo non esaustivo ma obbligatorio, alle seguenti attività e fornire i relativi *deliverable* minimi di Governance:

- **Gestione dei Comitati e dei SAL (Stati di Avanzamento Lavori):**
    - **organizzazione e gestione dei Comitati Direttivi e Strategici:** incontri da programmare in base alle esigenze e al *timing* del progetto (es. trimestrali o semestrali), finalizzati alla revisione del piano strategico di sicurezza, all'approvazione di *roadmap* a medio-lungo termine e alla valutazione dell'impatto delle nuove normative;
    - **conduzione e verbalizzazione dei SAL Executive (Direzionali):** incontri ad alta valenza strategica e decisionale, con la partecipazione del *management* e della Direzione della Stazione Appaltante e dell'HUB Sanitario, finalizzati alla revisione delle performance complessive, all'indirizzo strategico, all'approvazione dei piani di intervento prioritari e alla gestione delle eventuali criticità di alto livello. La verbalizzazione deve essere dettagliata e focalizzata sui punti decisionali. La frequenza a regime sarà mensile, ma potrebbero essere necessari ulteriori incontri durante le fasi iniziali dell'appalto o sulla base delle necessità della Stazione Appaltante;
    - **conduzione e verbalizzazione dei SAL Operativi:** riunioni a cadenza più frequente, dedicate all'analisi dettagliata dello stato di avanzamento delle attività operative, al monitoraggio degli indicatori chiave di performance (KPI), alla revisione dei *task* in corso e alla risoluzione delle problematiche tattiche. La frequenza a regime sarà settimanale.
    - **conduzione e verbalizzazione di incontri con gli Aggiudicatari del Lotto 2:** incontri focalizzati sul coordinamento tecnico, sulla risoluzione rapida di

impedimenti operativi, sull'allineamento delle procedure e sulla verifica dell'aderenza agli standard richiesti. La frequenza a regime sarà settimanale o ad ogni necessità.

- **Gestione delle azioni (Action Item) e delle azioni correttive e preventive (CAPA):**
  - **Redazione completa dei verbali:** ogni verbale di riunione, di qualsiasi livello (Executive, Operativo, Tecnico), dovrà includere una sezione dedicata all'identificazione chiara e univoca di tutte le azioni necessarie (*Action Item*).
  - **Assegnazione di responsabilità e *Deadline*:** per ciascuna azione, dovranno essere specificati il responsabile esecutivo (*owner*) e la data di completamento prevista (*deadline*), al fine di garantirne la tracciabilità.
  - **Tracciamento delle CAPA (Corrective and Preventive Actions):** implementazione di un processo strutturato per l'identificazione, l'analisi delle cause radice (*Root Cause Analysis*), la definizione, l'assegnazione e il monitoraggio costante delle **Azioni correttive e preventive (CAPA)**. Tali azioni dovranno essere attivate sistematicamente in risposta ad anomalie, disservizi o incidenti significativi riscontrati nella conduzione dei servizi, rilievi, non conformità o raccomandazioni emerse da audit interni o esterni eseguiti sugli Aggiudicatari dei servizi. Ogni azione dovrà essere tracciata al fine di garantire la visibilità in tempo reale sul suo stato di implementazione.

- **Analisi e valutazione degli strumenti di supporto:**

  - **Valutazione periodica e critica degli strumenti di mercato in uso:** l'Aggiudicatario dovrà condurre un'analisi periodica con cadenza almeno semestrale dell'efficienza e dell'allineamento tecnologico degli strumenti a supporto della Governance e delle operazioni del CSIRT Regionale. L'analisi dovrà proporre raccomandazioni per l'ottimizzazione o l'eventuale sostituzione degli stessi, garantendo l'adozione delle *best practice* di mercato, in via prioritaria ma non esclusiva, su piattaforme come:
    - **ITSM (IT Service Management):** Valutazione della capacità di gestione di incidenti, *request*, problemi e *change*.
    - **Mail e Document Management:** Verifica dell'adeguatezza degli strumenti per la comunicazione sicura e l'archiviazione controllata della documentazione.
    - **Piattaforme GRC (Governance, Risk, and Compliance):** Analisi dell'efficacia degli strumenti utilizzati per il monitoraggio della conformità normativa e la gestione dei rischi di sicurezza.

- **Supporto per ispezioni e audit:**

  - L'aggiudicatario dovrà supportare la Stazione Appaltante nel reperire rapidamente tutta la documentazione necessaria a dimostrare l'adempimento agli obblighi contrattuali e normativi, in particolare in caso di ispezioni, verifiche o audit da parte di enti regolatori o autorità di controllo.

### 2.3.1 Piano di adozione

L'Aggiudicatario dovrà definire un **piano di adozione** strutturato per il servizio di Governance, mirato a garantire una transizione fluida e una rapida messa a regime dei processi di controllo ed indirizzo. La Roadmap potrà essere articolata in più fasi che comprendano almeno le seguenti attività:

| Fase | Durata | Obiettivi e Attività Principali |
|---|---|---|
| Affiancamento iniziale | 0-3 mesi | Affiancamento del Fornitore uscente, verifica documentazione, formazione del team. |
| Avvio | 3-6 mesi | Avvio del presidio di Governance, organizzazione e convocazione dei Comitati (Strategico e Direttivo), presa in carico della suite tecnologica (Ticketing, BI, Repository, etc) e integrazione con i vari servizi, verifica e approvazione formale dei KPI/SLA/Penali relativi ai servizi, produzione prima reportistica. |
| Maturità Operativa e Controllo | 6-12 mesi | Messa a regime del controllo continuo sugli Aggiudicatari dei servizi del Lotto 2, reportistica avanzata, tracciamento sistematico di tutte le CAPA, esecuzione di audit, monitoraggio di tutti i servizi. |
| Specializzazione e Automazione | 12-45 mesi | Ottimizzazione e affinamento delle procedure di controllo. Revisione annuale della Security Strategy e del Risk Tolerance. Introduzione di automazioni nei processi di Reporting (BI) e di notifica Normativa (Alerting). Valutazione delle performance e predisposizione del "**Piano di trasferimento del Know-How**". |
| Affiancamento di fine fornitura | 45-48 mesi | Affiancamento del Fornitore entrante per il passaggio di consegne. |

### 2.3.2 Reportistica

Oltre alla reportistica richiesta nei paragrafi precedenti, l'Aggiudicatario dovrà produrre una reportistica periodica, basata sui dati derivanti dai KPI/SLA misurati e dalle evidenze raccolte, con l'obiettivo di fornire una visione chiara e decisionale allo *Strategic Management*.

Nello specifico dovranno essere prodotti e presentati alla Stazione Appaltante almeno i seguenti:

- **Report Mensile Operativo**: focalizzato sull'andamento tattico dei servizi. Include il dettaglio degli Action Item, lo stato di avanzamento delle attività e il rispetto degli SLA per tutti i servizi, l'analisi dei trend di incidenti e un *tracking* puntuale di tutte le CAPA attive.
- **Report Trimestrale Direzionale**: destinato al Comitato Direttivo e Strategico. Include l'analisi e l'andamento dei KRI (es. esposizione al rischio, compliance normativa). Offre cruscotti interattivi per il *benchmarking* e il confronto delle macro-aree regionali (es. Sanità vs Enti Strumentali) e raccomandazioni strategiche di investimento e priorità di intervento.

La Stazione Appaltante si riserva la facoltà di richiedere ulteriori report sulla base delle proprie necessità.

I dati riportati nella reportistica prodotta dovranno essere verificabili (ove possibile) anche all'interno della "**Piattaforma di Business Intelligence (BI) e monitoraggio**" (vedi capitolo 2.2 Modello Architetturale).

### 2.3.3 Figure professionali e metrica di dimensionamento e remunerazione

Per erogare il presente servizio il fornitore dovrà disporre delle competenze, esperienze e capacità richieste ai profili professionali indicati nel seguito che costituiranno un team mix con le percentuali di impiego di seguito indicate:

- Security Principal (profilo avanzato);
- Information Security Consultant Senior;
- Data Protection e IA Specialist (profilo avanzato);
- Risk Manager (profilo avanzato);
- Legal support Senior.

La metrica di dimensionamento del servizio di "Servizi di Governance, controllo e supporto normativo" del CSIRT regionale è: giorni/team mix.

La modalità di remunerazione del servizio di "Servizi di Governance, controllo e supporto normativo" del CSIRT regionale è: a tempo/spesa..

# Art 3 - LOTTO 2 - Servizi integrati

## 3.1 SOC, Incident Management e Cyber Threat Intelligence

### 3.1.1 Oggetto del servizio e architettura modulare del SOC

Il Servizio ha per oggetto l'erogazione dei servizi di Security Operations Center (SOC), Incident Management, Crisis Management e Cyber Threat Intelligence (CTI) a favore degli

Enti della Constituency ritenuti idonei alla fruizione di tali servizi, secondo il livello di maturità dimostrato.

La numerosità degli Enti della Costituency costituisce il perimetro massimo di erogazione dei servizi e non un valore di adesione garantito. L'adesione ai servizi avviene secondo le seguenti modalità, non alternative tra loro nel tempo:

- adesione piena — l'Ente è onboardato sulla Security Data Platform dell'Aggiudicatario, che ne raccoglie la telemetria, ne effettua il monitoraggio e la gestione degli incidenti e ne cura la distribuzione dell'intelligence;
- adesione secondo il Modello Enti Autonomi — l'Ente dispone di proprio SIEM/SOC e mantiene la responsabilità operativa del monitoraggio sul proprio perimetro; l'Aggiudicatario assicura le integrazioni minime previste dal presente articolo, la ricezione della telemetria conferita, la correlazione con gli altri Enti della Constituency e la distribuzione dell'intelligence, senza onboarding sulla Security Data Platform;
- mancata adesione — l'Ente, per carenza di strumenti o di risorse, non attiva il servizio; in tal caso nessuna prestazione è dovuta nei suoi confronti fino all'eventuale successiva adesione.

L'Aggiudicatario è tenuto a erogare i servizi a favore degli Enti che aderiscono, in qualunque delle modalità sopra indicate, senza che la mancata adesione di uno o più Enti costituisca titolo per la revisione delle condizioni contrattuali.

L'elenco degli Enti aderenti a ciascun servizio e la relativa modalità di adesione sono rilevati in fase di onboarding, recepiti nel Piano di Avvio del Servizio e aggiornati con cadenza almeno semestrale in sede di SAL. Le variazioni intervenute nel corso della durata contrattuale sono comunicate formalmente dalla Stazione Appaltante.

L'Aggiudicatario dovrà individuare e nominare, prima dell'avvio del servizio, un Service Manager quale unico punto di riferimento contrattuale e organizzativo per l'intero Servizio (SOC, Incident Management, Crisis Management e CTI), con i seguenti compiti e responsabilità:

- costituire il punto di escalation unico verso la stazione appaltante per qualsiasi criticità, contestazione o richiesta di chiarimento relativa al servizio, indipendentemente dall'Ente della Constituency coinvolto;
- presiedere, in rappresentanza dell'Aggiudicatario, il SAL mensile previsto con la governance regionale, garantendo la presentazione dei report KPI, lo stato di avanzamento delle milestone e l'andamento degli indicatori di qualità;
- assumere la responsabilità organizzativa delle comunicazioni formali verso la stazione appaltante, incluse le notifiche di incidenti di sicurezza che coinvolgano l'infrastruttura dell'Aggiudicatario (di cui all'indicatore BREACH), le richieste di proroga o le segnalazioni di criticità sulle milestone contrattuali;
- coordinare, in caso di attivazione della Crisis Management ai sensi del §3.1.5, il raccordo tra la War Room operativa dell'Aggiudicatario e i referenti della governance regionale, fungendo da interfaccia per le decisioni che eccedono l'autorità del singolo team SOC;
- garantire la continuità del ruolo per l'intera durata contrattuale; in caso di sostituzione del Service Manager, l'Aggiudicatario è tenuto a darne comunicazione formale alla

stazione appaltante con un preavviso di almeno 15 giorni lavorativi, salvo cause di forza maggiore documentate, garantendo un periodo di affiancamento con il nuovo Service Manager non inferiore a 5 giorni lavorativi;

- il nominativo del Service Manager, unitamente al relativo curriculum vitae, è comunicato alla stazione appaltante in sede di Piano di Presa in carico. La stazione appaltante si riserva la facoltà di richiedere un colloquio tecnico di approfondimento e, qualora il profilo non risulti adeguato, di richiederne la sostituzione, con le modalità e i tempi previsti per le altre figure professionali del servizio;
- il Service Manager non deve essere necessariamente una figura dedicata in via esclusiva al presente contratto, ma deve garantire una disponibilità adeguata a coprire le esigenze di coordinamento e reperibilità del servizio, comprensiva della partecipazione H24x7x365 alla Crisis Management in caso di incidente di Severità 1 (S1) (§2.1.5).

L'Aggiudicatario dovrà garantire l'evoluzione dell'attuale modello di gestione verso un approccio MxDR (Managed Extended Detection and Response) basato su infrastrutture con paradigma cloud, le quali dovranno obbligatoriamente possedere le qualificazioni rilasciate dall'Agenzia per la Cybersicurezza Nazionale (ACN) adeguate alla tipologia di dato trattato.

È fatto esplicito divieto di proporre soluzioni che inducano ad un vendor lock-in tecnologico o metodologico. A tal fine, l'architettura del servizio dovrà essere modulare, interoperabile e basata su standard aperti, con dati archiviati in formati non proprietari e artefatti — regole di correlazione, playbook, indicatori di compromissione — consegnabili e portabili al termine del contratto. Il servizio di Threat Intelligence dovrà integrarsi operativamente con il SOC e con la MISP Regionale, quale infrastruttura di condivisione degli IoC con gli Enti della Constituency e con il CSIRT Italia.

Gli Enti della Constituency dispongono in parte di agenti di raccolta log già installati presso le proprie infrastrutture, che costituiscono il punto di origine della telemetria di sicurezza; per gli Enti che ne risultino privi, la relativa installazione è a carico dell'Aggiudicatario nell'ambito della fase di onboarding. Allo stato attuale la raccolta e l'inoltro dei log avvengono mediante la tecnologia IBM QRadar, in regime di licenza proprietaria. In affiancamento a tale infrastruttura è preinstallata presso gli Enti una soluzione di raccolta open source basata su Logstash, destinata a sostituire progressivamente la componente QRadar.

All'avvio del servizio l'Aggiudicatario prenderà in carico l'infrastruttura nello stato in cui si trova e dovrà completare, per tutti gli Enti della Constituency, la transizione dalla tecnologia QRadar alla soluzione open source Logstash o analoga soluzione equivalente che eviti vincoli tecnologici verso uno specifico fornitore, con la conseguente dismissione della componente proprietaria in licenza, secondo le modalità e i termini di cui alle milestone M01 e M11 (§3.1.2). Il completamento della transizione è a carico dell'Aggiudicatario e non comporta oneri aggiuntivi per la stazione appaltante né per gli Enti.

Sui sistemi Microsoft degli Enti è presente l'agente di raccolta proprietario di QRadar, che l'Aggiudicatario dovrà sostituire con un agente che non determini vincoli tecnologici verso uno specifico fornitore (lock-in), in coerenza con i principi di neutralità tecnologica e anti-lock-in richiamati nel presente Capitolato.

L'Aggiudicatario dovrà predisporre e gestire una Security Data Platform (SDP) in grado di ricevere i flussi di log da tutti gli agenti degli Enti in modalità multitenant, garantendo in ogni momento la separazione logica e la tracciabilità dei dati per ente di origine. L'Aggiudicatario controllerà in modo centralizzato le installazioni dei log collector presso gli Enti.

Il perimetro di monitoraggio non è limitato alle infrastrutture on-premise degli Enti. La superficie di attacco della Constituency comprende, oltre ai sistemi ospitati nei datacenter fisici degli Enti, anche i servizi erogati in modalità cloud di cui gli Enti si avvalgono, quali servizi di posta elettronica e collaboration in cloud, sistemi di gestione delle identità in cloud, infrastrutture IaaS e PaaS presso cloud provider e applicativi verticali erogati in modalità SaaS. L'Aggiudicatario dovrà pertanto garantire la capacità di raccogliere, normalizzare e correlare nella Security Data Platform anche la telemetria di sicurezza proveniente da tali sorgenti cloud, mediante le opportune integrazioni, ove l'Ente disponga di servizi cloud nel proprio perimetro e ne autorizzi l'integrazione.

Il censimento delle sorgenti cloud effettivamente presenti presso ciascun Ente è condotto dall'Aggiudicatario nella fase di onboarding, in collaborazione con l'Ente e con la governance del servizio, e recepito nel Piano di Avvio del Servizio. L'integrazione delle sorgenti cloud individuate rientra nel canone del servizio e non comporta oneri aggiuntivi per la stazione appaltante né per gli Enti.

L'Aggiudicatario è libero di proporre l'architettura della SDP che ritiene più idonea al raggiungimento degli obiettivi del servizio, scegliendo tra le seguenti modalità:

- Modalità Cloud: la SDP è erogata interamente su infrastruttura cloud di un provider qualificato ACN. La raccolta dei log presso ciascun Ente avviene tramite la soluzione di raccolta opensource già preinstallata in loco, connessa alla SDP dell'Aggiudicatario secondo le modalità e i termini di cui alla milestone M11 e all'onboarding di cui a M01 (§3.1.2). L'Aggiudicatario è responsabile della gestione, manutenzione e aggiornamento della soluzione di raccolta per tutta la durata del contratto;
- Modalità Ibrida: la raccolta dei log avviene tramite agenti installati presso le infrastrutture degli Enti (on-premise), mentre l'elaborazione, la normalizzazione e lo storage dei log sono ospitati su infrastruttura cloud qualificata ACN;
- Modalità On-Premise: la SDP è interamente ospitata presso datacenter fisici, inizialmente presso l'Aggiudicatario e successivamente migrata presso il datacenter regionale indicato dalla stazione appaltante.

Indipendentemente dalla modalità architetturale scelta, la SDP deve garantire gli stessi livelli di servizio, gli stessi requisiti di sicurezza, la stessa separazione logica multitenant e la stessa portabilità degli artefatti previsti dal presente capitolato. La modalità scelta deve essere dichiarata nell'offerta tecnica e non può essere modificata nel corso del contratto senza accordo scritto della stazione appaltante.

Le tempistiche e le modalità di operatività definitiva della SDP dipendono dalla modalità architetturale dichiarata in offerta:

- Modalità Cloud: la SDP è operativa in modalità definitiva sin dall'avvio del servizio; non è prevista migrazione verso il datacenter regionale. L'Aggiudicatario deve garantire

che la piattaforma sia erogata da datacenter ubicati nel territorio dell'Unione Europea, con certificazioni di sicurezza adeguate alla classificazione dei dati trattati (almeno ISO/IEC 27001) e conformità al Regolamento UE 2016/679 (GDPR). I datacenter e le infrastrutture cloud utilizzate per l'erogazione del servizio devono soddisfare i requisiti ambientali ex ante previsti dalla normativa DNSH (Do No Significant Harm) applicabile alle soluzioni cloud (con riferimento alla Scheda n. 6 della circolare RGS n. 22 del 14 maggio 2024 o successive modifiche); il fornitore è tenuto a fornire la relativa documentazione di conformità prima dell'avvio del servizio e a mantenerla aggiornata per tutta la durata contrattuale. La stazione appaltante non è tenuta ad acquisire o gestire alcuna infrastruttura fisica a tal fine.

- Modalità Ibrida: i collector on-premise presso gli Enti sono attivi sin dall'avvio del servizio. La SDP cloud deve essere operativa in modalità definitiva entro 6 mesi dalla data di avvio del servizio. Il mancato completamento entro tale termine non comporta l'applicazione immediata delle penali: è prevista una franchigia di 3 mesi (dal settimo al nono mese dall'avvio). Le penali si applicano integralmente a partire dal decimo mese dall'avvio del servizio.

- Modalità On-Premise: nella fase iniziale, la SDP potrà essere ospitata presso l'infrastruttura dell'Aggiudicatario. Entro 9 mesi dalla data di avvio del servizio, l'Aggiudicatario dovrà completare la migrazione della piattaforma presso il datacenter regionale indicato dalla stazione appaltante, senza interruzione del servizio e senza perdita di dati. Il mancato completamento entro tale termine non comporta l'applicazione immediata delle penali: è prevista una franchigia di 3 mesi (dal decimo al dodicesimo mese dall'avvio). Le penali si applicano integralmente a partire dal tredicesimo mese dall'avvio del servizio.

I dati contenuti nella SDP rimangono in ogni momento di esclusiva proprietà della Regione e potranno essere trattati dall'Aggiudicatario esclusivamente per le finalità previste dal contratto.

Per la modalità On-Premise, al termine del contratto, la Security Data Platform deve essere di esclusiva disponibilità e titolarità della Regione. Al termine del contratto, l'accesso dell'Aggiudicatario alla piattaforma è revocato.

Per le modalità Cloud e Ibrida, al termine del contratto si applica la seguente sequenza obbligatoria:

- Entro 30 giorni dalla notifica di termine contratto (fase di esportazione): l'Aggiudicatario è tenuto a esportare integralmente i dati, le regole di correlazione, i playbook e tutti gli artefatti prodotti nel corso del contratto verso un'infrastruttura indicata dalla stazione appaltante, in un formato concordato idoneo a consentire il trasferimento e il riutilizzo degli stessi. Al termine dell'esportazione l'Aggiudicatario ne dà comunicazione formale alla stazione appaltante;

- Dal giorno 31 al giorno 60 dalla notifica di termine contratto (grace period): i dati rimangono disponibili sulla propria infrastruttura cloud, senza oneri aggiuntivi per la stazione appaltante, al fine di consentire la verifica della completezza dell'esportazione e il recupero di eventuali elementi mancanti;

- Entro il giorno 60 dalla notifica di termine contratto (fase di cancellazione): l'Aggiudicatario procede alla cancellazione certificata di tutti i dati della propria infrastruttura cloud, fornendo idonee garanzie documentali dell'avvenuta cancellazione e della definitiva inaccessibilità dei dati. La stazione appaltante o soggetti terzi da essa designati possono richiedere di eseguire verifiche in merito entro i 30 giorni successivi alla cancellazione.

Per la modalità On-Premise, al termine del contratto l'accesso dell'Aggiudicatario alla Security Data Platform è revocato; i dati restano nella piena disponibilità della stazione appaltante senza necessità di esportazione. Si applica comunque il grace period di 30 giorni dalla notifica di termine durante il quale l'Aggiudicatario garantisce il supporto tecnico alla stazione appaltante per il passaggio di consegne, senza oneri aggiuntivi.

In tutti i casi e per tutte le modalità architetturali, i dati, le regole di correlazione, i playbook e tutti gli artefatti prodotti nel corso del contratto rimangono nella piena disponibilità della stazione appaltante al termine del contratto.

In conformità con le raccomandazioni dell'Agenzia per la Cybersicurezza Nazionale in materia di continuità operativa delle infrastrutture critiche, la Security Data Platform dovrà essere progettata per garantire la continuità del servizio anche in caso di indisponibilità del sito primario di erogazione. I requisiti di continuità operativa sono differenziati per modalità architetturale:

- Modalità On-Premise e Ibrida: l'Aggiudicatario dovrà prevedere la replica dei dati della SDP verso il datacenter secondario regionale indicato dalla stazione appaltante, con modalità e frequenza di sincronizzazione coerenti con gli obiettivi di RPO e RTO dichiarati nel Business Continuity Plan di cui alla milestone M14. La replica deve essere garantita sulla collocazione pro-tempore della SDP, sia essa provvisoria (presso l'infrastruttura dell'Aggiudicatario, in attesa del completamento di M12) o definitiva (presso il datacenter regionale primario): il completamento di M15 non è subordinato al completamento di M12 ed è dovuto entro 6 mesi dall'avvio, indipendentemente dallo stato di avanzamento della migrazione della SDP verso il datacenter regionale. Qualora, al raggiungimento del termine di M15, la SDP si trovi ancora presso l'infrastruttura provvisoria dell'Aggiudicatario, la replica verso il datacenter secondario regionale dovrà comunque essere attiva e successivamente riallineata, senza soluzione di continuità, al momento del completamento della migrazione. L'Aggiudicatario è tenuto a documentare l'architettura di replica nel BCP e a effettuare almeno un test annuale di failover, con esito comunicato alla stazione appaltante.
- Modalità Cloud: in luogo della replica verso il datacenter secondario regionale, l'Aggiudicatario dovrà garantire una soluzione di Business Continuity e Disaster Recovery interamente cloud, con RPO e RTO dichiarati nel BCP e coerenti con la natura del servizio. La soluzione BC/DR cloud deve prevedere ridondanza geografica su almeno due regioni cloud distinte, entrambe ubicate nel territorio dell'Unione Europea. L'Aggiudicatario è tenuto a documentare l'architettura BC/DR nel BCP e a effettuare almeno un test annuale di failover, con esito comunicato alla stazione appaltante. La soluzione BC/DR proposta è oggetto di valutazione tecnica ai sensi del criterio A.1 della rubrica di aggiudicazione.

La capacità di ingestione del servizio è dimensionata sulla base del valore medio di telemetria prodotta da ciascun ente, espresso in Events Per Second (EPS) o in volume di dati (TB/giorno), a seconda della tecnologia adottata dall'Aggiudicatario. Il valore attuale, alla data di stesura del documento, per tutti gli enti coperti dal servizio SOC offerto dal CERT è stimato attorno ai 85.000 EPS (equivalenti a circa 210TB/mese di traffico grezzo). La capacità complessiva garantita dal sistema è calcolata come somma dei valori medi di ciascun ente, maggiorata di un margine di picco globale del 30%. Non è ammesso un modello di dimensionamento che sommi i valori massimi individuali di ciascun ente.

Il volume di telemetria effettivamente rilevato è misurato dal sistema di monitoraggio della Security Data Platform, i cui dati costituiscono il riferimento ufficiale per la fatturazione.

In caso di superamento improvviso e non strutturale della capacità garantita — dovuto ad esempio a un incidente in corso, a una campagna di attacco su più enti o a un picco anomalo di telemetria — il servizio non dovrà in nessun caso essere interrotto. L'Aggiudicatario dovrà garantire la continuità del monitoraggio e della detection anche in condizioni di sovraccarico, accettando se necessario una degradazione controllata che potrà tradursi nella perdita temporanea degli eventi in eccesso rispetto alla capacità garantita, ma mai nell'interruzione del servizio verso gli Enti. Il verificarsi di tale situazione dovrà essere notificato immediatamente alla stazione appaltante con indicazione del volume in eccesso, della durata stimata e delle azioni intraprese.

Qualora il superamento si ripeta per più di **3 giorni consecutivi** per il medesimo Ente, ciò costituisce evidenza di un dimensionamento strutturalmente inadeguato. In tal caso l'Aggiudicatario è tenuto a notificarlo entro 24 ore alla stazione appaltante e ad avviare immediatamente la procedura di ridimensionamento straordinario per quell'Ente. Il nuovo valore medio atteso dovrà essere concordato e attivato entro **5 giorni lavorativi** dalla prima notifica. Il mancato completamento del ridimensionamento entro tale termine comporta l'applicazione delle penali previste nell'Allegato C1 - Indicatori di qualità.

Per tutta la durata contrattuale, l'Aggiudicatario è tenuto a mantenere l'intera infrastruttura dedicata all'erogazione del servizio in condizioni di piena operatività, aggiornamento e sicurezza. Gli interventi di manutenzione devono essere concordati con la stazione appaltante con un preavviso minimo di 15 giorni lavorativi, pianificati in fasce orarie a basso impatto operativo e comunicati preventivamente a tutti gli Enti della Constituency interessati. Per gli aggiornamenti urgenti di sicurezza il preavviso è ridotto a 24 ore.

In caso di incidente di sicurezza subito dall'Aggiudicatario che coinvolga dati degli Enti, l'Aggiudicatario è tenuto a notificare la stazione appaltante entro 24 ore dall'identificazione dell'incidente. In caso di uscita di un singolo Ente dalla Constituency, l'Aggiudicatario è tenuto a garantire l'esportazione integrale dei dati in formato aperto entro 30 giorni e la cancellazione certificata entro 60 giorni.

L'architettura dovrà essere differenziata in base al gruppo di appartenenza e al livello di maturità di ciascun Ente, articolandosi nei seguenti scenari:

- **Modello Enti Autonomi:** modello destinato agli Enti dotati di proprio SIEM/SOC, basato su un'architettura disaccoppiata dalla raccolta e normalizzazione dei log gestita centralmente. In questo modello l'Ente mantiene la piena autonomia operativa del

proprio SOC, ma è tenuto a garantire un livello minimo di integrazione con il CERT regionale secondo tre direttrici:

- **Condivisione degli IoC:** gli IoC rilevati dal SOC dell'Ente devono essere pubblicati sulla MISP Regionale in formato STIX 2.1 tramite TAXII 2.1, con cadenza almeno giornaliera per gli IoC ad alta priorità, al fine di consentire la distribuzione automatica verso gli altri Enti della Constituency;
- **Visibilità operativa:** l'Ente deve esporre al CERT regionale, tramite API REST documentata, lo stato aggregato del proprio servizio SOC: numero di alert aperti, ticket in lavorazione, ticket chiusi nel periodo, livello di copertura MITRE ATT&CK aggiornato; questi dati devono confluire nella dashboard operativa del CERT regionale per garantire una visione unitaria dello stato di sicurezza dell'intera constituency, inclusi gli Enti autonomi;
- **Ricezione e gestione dei ticket:** l'Ente deve dimostrare di prendere in carico i ticket di sicurezza generati o inoltrati dal CERT regionale entro i tempi previsti dal proprio accordo di servizio, con rendicontazione mensile degli esiti verso il CERT regionale; il mancato riscontro sistematico costituisce elemento di valutazione nell'ambito del SAL mensile;

Il fornitore del servizio SOC regionale è tenuto a supportare gli Enti Autonomi nel processo di integrazione, fornendo le specifiche tecniche delle API e dei feed MISP necessari, e a segnalare al CERT regionale eventuali Enti che non rispettino gli obblighi minimi di integrazione;

- **Central SOC** (Enti Medi): architettura centralizzata "all-in-one" multi-entità;

- **Medical SOC** (Enti Sanitari — Gruppo 1): componente specializzata per gli enti sanitari e socio-sanitari;

- **Connettività diretta:** modello destinato agli Enti di piccole dimensioni che, per limiti infrastrutturali od organizzativi, non dispongono di una soluzione di raccolta locale; la telemetria viene trasmessa direttamente alla SDP tramite connessione diretta e sicura, con il minor impatto possibile sull'infrastruttura e sull'operatività dell'Ente. L'Aggiudicatario può proporre tecnologie alternative a quella standard, a condizione che garantiscano un impatto sull'Ente non superiore a quello della soluzione di riferimento, previa approvazione della stazione appaltante;

- **Modello PSR (Enti Piccoli):** modello destinato agli Enti piccoli in fase di trasferimento verso il Polo Strategico Regionale, con architettura di raccolta e monitoraggio adeguata al contesto infrastrutturale del PSR.

### 3.1.2 Obblighi di avvio e milestone iniziali

Il presente articolo definisce gli adempimenti che l'Aggiudicatario è tenuto a completare entro termini perentori decorrenti dalla data di avvio del servizio. Per avvio di servizio si intende la data in cui il servizio sarà totalmente in mano all'Aggiudicatario. Le milestone di avvio costituiscono obblighi a consumazione: si intendono soddisfatti una volta adempiuti e verificati dalla stazione appaltante. Il mancato rispetto dei termini comporta l'applicazione delle penali previste nell'Allegato C1 - Indicatori di qualità.

| # | Milestone | Termine | Modalità di verifica |
|---|---|---|---|
| M01 | Completamento dell'onboarding sequenziale di tutti gli Enti che aderiscono al servizio in modalità piena, come individuati nel Piano di Avvio del Servizio, sulla nuova SDP, tramite connessione della soluzione opensource preinstallata e swap della sonda preesistente per ciascun Ente; per gli Enti che aderiscono secondo il Modello Enti Autonomi la milestone si intende adempiuta con l'attivazione delle integrazioni minime di cui al §3.1.1 secondo quanto predisposto in M11. Il servizio SOC H24x7x365 e i relativi SLA inderogabili di cui al §3.1.5 sono operativi per ciascun Ente a partire dal completamento del suo onboarding; M01 certifica il raggiungimento della copertura completa dell'intera Constituency, non l'inizio del servizio, che avviene progressivamente ente per ente. | 90 giorni | Verifica funzionale tramite test di notifica su tutti gli Enti; verifica che tutti gli Enti risultino attivi sulla nuova SDP con ingestione confermata |
| M02 | Attivazione e verifica della connettività MISP Regionale con il CSIRT Italia | 15 giorni | Test di scambio IoC in formato STIX 2.1 / TAXII 2.1 con esito documentato |
| M03 | Attivazione della dashboard operativa in tempo reale con autenticazione MFA | 30 giorni | Verifica di accesso da parte dei referenti tecnici della stazione appaltante |
| M04 | Prima popolazione del CMDB per ciascun ente della constituency | 60 giorni | Consegna del CMDB in formato aperto e validazione con i referenti degli enti |
| M05 | Ricezione, validazione e integrazione nel CMDB degli SBOM forniti dal servizio di Vulnerability Management. L'integrazione presuppone il completamento della prima popolazione del CMDB di cui a M04; qualora gli SBOM siano resi disponibili dal servizio VM prima del completamento di M04, il termine di M05 decorre dalla più tardiva tra la data di messa a disposizione degli SBOM e la data di completamento di M04. | 60 giorni dalla messa a disposizione degli SBOM da parte del servizio VM (o dal completamento di M04, se successivo) | Verifica dell'integrazione nel CMDB da parte della stazione appaltante; consegna del registro delle lacune segnalate al VM |

| # | Milestone | Termine | Modalità di verifica |
|---|---|---|---|
| M06 | Attivazione dell'integrazione tra il SOAR e il ticketing system adottato dalla governance | 15 giorni | Test di apertura automatica di ticket su scenari simulati, con esito documentato |
| M07 | Consegna del piano di tuning iniziale delle regole di correlazione con mappatura MITRE ATT&CK e baseline dei falsi positivi attesi | 45 giorni | Validazione da parte del team CERT regionale in sessione dedicata |
| M08 | Prima sessione di formazione con il personale interno del CERT regionale e i referenti degli enti | 60 giorni | Verbale di svolgimento firmato dai partecipanti |
| M09 | Consegna del catalogo dei playbook di risposta iniziali (phishing, ransomware, accessi anomali) | 45 giorni | Validazione formale da parte della stazione appaltante |
| M10 | Prima sessione di threat hunting proattivo con report delle ipotesi investigate | 90 giorni | Consegna del report in formato concordato e presentazione al CERT regionale |
| M11 | Predisposizione e collaudo della Security Data Platform per la ricezione multitenant dei flussi log, con verifica della separazione logica su un campione rappresentativo di almeno 3 Enti pilota, selezionati in accordo con la stazione appaltante tra le diverse tipologie architetturali presenti nella Constituency. La milestone attesta la piena capacità tecnica della SDP di ricevere e distinguere correttamente i flussi di tutti gli Enti della Constituency, quale condizione abilitante per l'avvio dell'onboarding sequenziale di tutti gli Enti di cui a M01. Il termine si applica uniformemente a tutte le modalità architetturali. | 45 giorni dall'avvio | Test di ingestione con dataset di prova su almeno 3 Enti pilota; verifica della separazione logica multitenant |
| M12 | Operatività definitiva della Security Data Platform: per la modalità Cloud, la SDP è già operativa in modo definitivo all'avvio (M12 soddisfatta al giorno 0); per la modalità Ibrida, completamento della configurazione definitiva della | Modalità-dipendente (vedi §3.1.1) | Collaudo congiunto: verifica della disponibilità del servizio, integrità dei dati storici e operatività di tutti i sistemi integrati (SOAR, MISP, CMDB, dashboard) |

| # | Milestone | Termine | Modalità di verifica |
|---|---|---|---|
| | SDP cloud entro 6 mesi; per la modalità On-Premise, completamento della migrazione della SDP presso il datacenter regionale entro 9 mesi . | | |
| M13 | Consegna della documentazione tecnica descrittiva dei dati degli Enti presenti sulla Security Data Platform, con indicazione della relativa ubicazione, delle modalità di trattamento e delle misure di sicurezza adottate | 15 giorni lavorativi dal completamento della M12 | Validazione formale da parte del team tecnico della stazione appaltante |
| M14 | Consegna del Business Continuity Plan del servizio SOC con RTO e RPO dichiarati per ciascun componente critico dell'infrastruttura | 30 giorni | Validazione formale da parte della stazione appaltante; il BCP deve includere scenari di failover, procedure di ripristino e responsabilità operative documentate |
| M15 | Attivazione della soluzione BC/DR della Security Data Platform: per le modalità On-Premise e Ibrida, attivazione della replica verso il datacenter secondario regionale con verifica della consistenza dei dati e test di failover; per la modalità Cloud, attivazione della soluzione BC/DR cloud con ridondanza geografica su almeno due regioni EU distinte e test di failover | 6 mesi | Collaudo congiunto con la stazione appaltante: verifica della soluzione BC/DR attiva, test di failover con ripristino del servizio entro i tempi RTO dichiarati nel BCP e verifica dell'integrità dei dati |
| M16 | Attivazione delle integrazioni minime per gli Enti Autonomi: feed MISP in STIX 2.1, API di visibilità operativa e canale di ricezione ticket dal CERT regionale | 90 giorni per ciascun Ente Autonomo dalla data di adesione al modello | Test di pubblicazione IoC su MISP; verifica della raggiungibilità e aggiornamento dell'API di visibilità operativa; test di invio e ricezione ticket dal CERT regionale; esito documentato per ciascun Ente |
| M17 | Completamento del censimento passivo iniziale dei dispositivi IoMT e prima popolazione dell'inventario clinico integrato con il CMDB, per l'Azienda Sanitaria individuata dalla stazione appaltante ai fini della sperimentazione Medical SOC di cui al §3.1.6 | 90 giorni dalla data di individuazione dell'Ente sanitario pilota da parte della stazione appaltante | Verifica dell'inventario consegnato; validazione congiunta con i referenti clinici e tecnici dell'Ente sanitario dell'approccio passivo adottato |

| # | Milestone | Termine | Modalità di verifica |
|---|---|---|---|
| M18 | Accreditamento alla piattaforma HyperSOC dell'Agenzia per la Cybersicurezza Nazionale, con attivazione del canale di trasmissione degli eventi di sicurezza anonimizzati e di ricezione delle regole di detection distribuite da ACN | 30 giorni dall'avvio | Evidenza documentale dell'accreditamento rilasciata da ACN; verifica dei log di trasmissione degli eventi verso HyperSOC; test di ricezione di una regola di detection in formato standard |
| M19 | Attivazione del monitoraggio del Deep Web e Dark Web per la rilevazione di data leakage, credential leakage e domain squatting riferiti agli Enti della Constituency e ai loro domini istituzionali | 6 mesi dall'avvio | Report di attivazione con descrizione della metodologia e degli strumenti adottati; evidenza delle prime segnalazioni prodotte per gli Enti |

Parallelo operativo in caso di subentro o migrazione

La presa in carico del servizio avviene in regime di subentro al fornitore precedente. Completata la predisposizione e il collaudo della SDP (M11, entro 45 giorni dall'avvio), l'Aggiudicatario procede all'onboarding sequenziale di tutti gli Enti della Constituency (attualmente pari a 41), da completare entro il termine di 90 giorni dall'avvio del servizio previsto in M01. Per ciascun Ente l'onboarding avviene tramite swap dell'indirizzo IP dalla sonda preesistente alla soluzione opensource già installata in loco e connessa alla SDP, garantendo la continuità della copertura di monitoraggio senza interruzioni per il singolo Ente; durante il periodo di onboarding complessivo, gli Enti non ancora migrati restano coperti dalla soluzione del fornitore uscente. Tutti gli interventi di switch devono essere effettuati al di fuori degli orari di operatività ordinaria dell'Ente, salvo accordo diverso. Le modalità di coordinamento con ciascun Ente, incluso il relativo cronoprogramma di onboarding, sono definite nel Piano di Avvio del Servizio e approvate dalla stazione appaltante.

Il termine della milestone M15 (6 mesi) decorre dall'avvio del servizio; il mancato completamento è soggetto alle penali previste dall'Allegato C1 - Indicatori di qualità, senza franchigia. La milestone M16 si applica individualmente per ciascun Ente che aderisca al Modello Enti Autonomi nel corso della durata contrattuale; il termine di 90 giorni decorre dalla data di formalizzazione dell'adesione da parte dell'Ente.

Entro 15 giorni dal completamento di tutte le milestone M01-M15, M18 e M19, la stazione appaltante effettua un collaudo di avvio complessivo del servizio, con verifica funzionale degli SLA operativi, delle integrazioni tra i sistemi, della copertura MITRE ATT&CK rispetto alla baseline dichiarata in offerta e della disponibilità degli SBOM. L'esito è documentato in un verbale sottoscritto da entrambe le parti. La milestone M16, in quanto legata all'adesione volontaria e progressiva dei singoli Enti al Modello Enti Autonomi nel corso dell'intera durata contrattuale, non rientra nel perimetro del presente collaudo di avvio complessivo: per ciascun Ente che aderisca al modello, il collaudo è effettuato separatamente entro i termini previsti dalla milestone M16 stessa.

### 3.1.3 SOC e Incident Management assistito (End-to-End)

Il servizio SOC non dovrà limitarsi al mero monitoraggio e correlazione dei log provenienti dai sistemi degli Enti, ma dovrà configurarsi come un servizio di Incident Management assistito End-to-End.

**REQUISITI DA ATTUARE ALL'AVVIO DEL SERVIZIO**

**Operatività e monitoraggio**

- operatività H24x7x365 per il monitoraggio, il triage e la segnalazione degli eventi;
- adozione della tassonomia degli eventi e degli incidenti di sicurezza TC-ACN definita dall'Agenzia per la Cybersicurezza Nazionale (disponibile sul sito istituzionale ACN), rigorosamente allineata al D.Lgs. 138/2024 (NIS2) e alla Legge 90/2024; la tassonomia TC-ACN è vincolante sia per la classificazione interna degli eventi sia per le notifiche verso le Autorità competenti, al fine di agevolare lo scambio di informazioni a livello nazionale attraverso un lessico comune e garantire l'armonizzazione con le tassonomie internazionali in materia di cybersecurity;
- accreditamento obbligatorio alla piattaforma HyperSOC dell'Agenzia per la Cybersicurezza Nazionale (ACN), da completare entro 30 giorni dall'avvio del servizio; l'accreditamento è finalizzato a: (a) fornire ad ACN informazioni sugli eventi di sicurezza rilevati nella Constituency, opportunamente anonimizzati, per potenziare le capacità di monitoraggio e analisi a livello nazionale; (b) ricevere in input regole di detection in formati standard (YARA, SIGMA, Snort) distribuite da ACN; la mancata attivazione dell'accreditamento entro il termine indicato costituisce inadempimento soggetto alle penali previste nell'Allegato C1 - Indicatori di qualità;
- dashboard operativa in tempo reale, accessibile al CSIRT regionale e a tutti gli Enti della Constituency, con visibilità su alert attivi, stato degli Enti e copertura delle regole MITRE; deve essere esposta via web con autenticazione MFA e non limitata al portale del fornitore o alla dashboard fornita dalla governance;
- mappatura MITRE ATT&CK obbligatoria: ogni alert generato deve essere mappato alle tattiche e tecniche MITRE ATT&CK (Enterprise + ICS ove pertinente); il report mensile deve includere la coverage matrix aggiornata;

**Detection e qualità degli alert**

- SOC "AI Augmented": introduzione di scenari supportati dall'Intelligenza Artificiale per il triage, l'arricchimento degli eventi e il suggerimento di azioni di contenimento, con l'obiettivo di ridurre il carico manuale e i falsi positivi; il comportamento algoritmico dovrà essere costantemente monitorato e verificabile;
- modelli ML spiegabili: i modelli di machine learning utilizzati per la detection devono essere documentati e spiegabili — non sono ammissibili approcci di tipo black box non giustificabili — e l'Aggiudicatario deve fornire la logica sottostante a ogni alert complesso;

- implementazione di regole di correlazione basate su signature e indicatori noti, con copertura minima del 40% delle tecniche MITRE ATT&CK Enterprise verificabile tramite ATT&CK Navigator in sede di collaudo;
- integrazione con CMDB e Vulnerability Management: implementazione e utilizzo di un CMDB accurato per ciascun Ente, al fine di correlare gli eventi rilevati con le vulnerabilità note e prioritizzare i rischi in modo contestuale;
- contributo alla popolazione del CMDB centralizzato gestito dalla governance, per quanto di competenza del servizio SOC, con i dati rilevati nel corso delle attività di monitoraggio e incident management;
- correlazione laterale e propagazione delle minacce tra enti: il sistema di detection dovrà essere in grado di correlare eventi e pattern di attacco rilevati su un Ente con la situazione di sicurezza degli altri Enti della Constituency; qualora venga identificato un pattern di attacco, un indicatore di compromissione o un comportamento anomalo su un Ente, tale informazione dovrà essere automaticamente valorizzata per anticipare, rilevare o prevenire minacce analoghe sugli altri Enti, attraverso l'aggiornamento delle regole di detection attive, la distribuzione di alert preventivi e l'arricchimento del contesto CTI; il sistema dovrà documentare mensilmente i casi in cui la correlazione laterale ha contribuito alla prevenzione o al rilevamento anticipato di un incidente;
- utilizzo degli SBOM (Software Bill of Materials) forniti dal servizio di Vulnerability Management come strumento di correlazione tra vulnerabilità note (CVE) e asset effettivamente esposti; il SOC dovrà integrare gli SBOM nel CMDB di ciascun Ente e utilizzarli per la prioritizzazione degli alert, consentendo di rispondere con precisione e tempestività all'emergere di nuove minacce.

**Automazione, orchestrazione e portabilità**

- automazione prudente (SOAR): utilizzo di tecnologie SOAR per l'orchestrazione e la risposta automatizzata, vincolata a rigorosi limiti autorizzativi e di controllo definiti da ciascun ente; si precisa che la correlazione laterale tra enti genera automaticamente alert preventivi e aggiornamento delle regole di detection, mentre le azioni di risposta operative rimangono soggette ai normali limiti autorizzativi SOAR;
- integrazione bidirezionale con la Security Data Platform: il SOAR deve interrogarla in tempo reale per l'arricchimento del contesto degli eventi, senza richiedere la duplicazione dei dati sulla piattaforma del fornitore;
- API REST documentata e aperta: tutti i workflow di automazione devono essere attivabili tramite API standard con documentazione obbligatoria in formato Swagger/OpenAPI 3.x;
- integrazione con i sistemi esistenti: il SOAR deve integrarsi con il sistema di ticketing adottato dalla governance;
- playbook di risposta standard: il fornitore deve sviluppare e mantenere playbook specifici per le casistiche più comuni nella Pubblica Amministrazione, tra cui phishing, ransomware e accessi anomali su portali istituzionali;

- portabilità degli artefatti: tutte le regole di correlazione sviluppate nell'arco del contratto devono essere esprimibili in formato aperto (SIGMA, YARA-L o equivalente documentato con conversione bidirezionale dimostrabile tramite strumenti standard) e consegnate integralmente al termine del contratto; i playbook SOAR devono essere esportabili in formato aperto (CACAO, STIX Courses of Action o script documentati); i log devono essere archiviati in formati aperti su storage esportabile verso infrastruttura dell'amministrazione (S3-compatibile o equivalente documentato); gli eventi devono essere normalizzati secondo uno schema aperto interoperabile (OCSF o equivalente con mappatura pubblica e conversione dimostrabile, quale ASIM o UDM); al termine del contratto, indipendentemente dalla modalità architetturale adottata, l'amministrazione deve poter riprendere regole di correlazione, playbook e intelligence in formato aperto, senza dipendenza dalla piattaforma del fornitore uscente;

**Gestione degli incidenti e KPI**

- KPI mensili obbligatori: MTTD, MTTR, tasso di falsi positivi, copertura MITRE ATT&CK per ente e numero di IoC condivisi; i dati devono essere esportabili in formato CSV/JSON;
- report di incidente strutturato: ogni incidente di Severità 1 (S1) o Severità 2 (S2) deve produrre una Relazione post-risoluzione entro cinque giorni lavorativi dalla chiusura dell'incidente, contenente timeline, root cause, IoC rilevati, eventuali azioni di remediation raccomandate. il report del SOC costituisce la base documentale a supporto di tale adempimento normativo;
- supporto agli Enti per gli obblighi di notifica al CSIRT Italia: gli obblighi di notifica degli incidenti significativi di cui all'art. 25 del D.Lgs. 138/2024 restano in capo a ciascun Ente nella propria qualità di soggetto NIS. L'Aggiudicatario è tenuto a supportare l'Ente nella predisposizione delle notifiche da trasmettere attraverso il portale dell'Agenzia per la Cybersicurezza Nazionale, fornendo tempestivamente gli elementi informativi tecnici necessari secondo i seguenti termini, computati dalla qualificazione dell'incidente come potenzialmente significativo da parte del SOC:
    - pre-notifica (art. 25, comma 5, lettera a) — 24 ore): l'Aggiudicatario mette a disposizione dell'Ente, entro 8 ore, gli elementi utili alla pre-notifica, con indicazione, ove desumibile, se l'incidente possa ritenersi il risultato di atti illegittimi o malevoli e se possa avere un impatto transfrontaliero;
    - notifica (art. 25, comma 5, lettera b) — 72 ore): l'Aggiudicatario mette a disposizione dell'Ente, entro 48 ore, gli elementi utili alla notifica, comprensivi dell'aggiornamento delle informazioni già trasmesse, della valutazione iniziale dell'incidente con indicazione della gravità e dell'impatto e degli indicatori di compromissione rilevati;
    - relazione intermedia (art. 25, comma 5, lettera c): ove il CSIRT Italia ne faccia richiesta, l'Aggiudicatario fornisce gli elementi tecnici necessari entro 3 giorni lavorativi dalla comunicazione dell'Ente.

- audit log degli amministratori: tutte le attività degli Amministratori di Sistema dell'Aggiudicatario sulla Security Data Platform devono essere registrate in un audit log immutabile, conservato per almeno 12 mesi e reso disponibile alla stazione appaltante su richiesta entro 24 ore;

**Governance e trasferimento di competenze**

- SAL mensile: riunione operativa obbligatoria tra l'Aggiudicatario, Regione del Veneto e la governance del CSIRT (Aggiudicatario del Lotto 1), convocata dalla governance stessa con cadenza mensile; l'ordine del giorno deve includere obbligatoriamente: l'andamento del servizio con analisi dei KPI del periodo, gli spunti di miglioramento emersi, e il resoconto delle attività di manutenzione dell'infrastruttura effettuate nel mese — con indicazione degli aggiornamenti applicati, delle CVE trattate e delle eventuali vulnerabilità rilevate e rimediate; l'Aggiudicatario è tenuto a produrre e consegnare un verbale scritto entro 5 giorni lavorativi dalla riunione;
- analisi orientata al miglioramento continuo: devono essere organizzate sessioni periodiche con i referenti della Constituency e con la governance, finalizzate all'ottimizzazione del sistema, alla riduzione dei falsi positivi e al supporto nell'implementazione di eventuali modifiche o migliorie, anche attraverso incontri dedicati in presenza;

**REQUISITI DA ATTUARE ENTRO I TERMINI INDICATI**

I seguenti requisiti non sono richiesti al momento dell'avvio del servizio, ma devono essere raggiunti entro i termini indicati, con le modalità definite nell'articolo dedicato alle milestone.

- **entro 12 mesi** — rilevamento basato su comportamento (UEBA): il sistema deve includere l'analisi comportamentale di utenti ed entità per rilevare anomalie non coperte da signature statiche, con metriche sui falsi positivi verificate in sede di verifica periodica;
- **entro 12 mesi** — copertura MITRE ATT&CK: incremento della copertura delle tecniche MITRE ATT&CK Enterprise fino ad almeno il 60%, verificabile tramite ATT&CK Navigator;
- **entro 12 mesi** — tuning collaborativo delle regole: sessioni mensili di tuning con il team interno e con i responsabili del servizio presso gli Enti, con esplicito trasferimento di know-how;
- **entro 12 mesi** — penetration test annuale sull'infrastruttura SOC condotto da soggetto terzo qualificato ACN, con consegna del report entro 30 giorni e remediation delle vulnerabilità critiche entro 30 giorni dal report;
- **entro 6 mesi** — console di gestione centralizzata dei log collector: l'Aggiudicatario dovrà predisporre uno strumento di fleet management che consenta la gestione remota centralizzata di tutti i collector installati presso gli Enti della Constituency, con funzionalità minime di monitoraggio dello stato di salute di ciascun collector, aggiornamento remoto della configurazione, distribuzione centralizzata degli aggiornamenti software e alerting in caso di collector non raggiungibile o in errore; la

console dovrà essere accessibile al CSIRT regionale con profilo di sola lettura per il monitoraggio, e al fornitore con profilo operativo per la gestione;

- **entro 12 mesi** - tecnologie deceptive (honeypot e honeynet): deployment di asset decoy all'interno delle reti degli Enti per intercettare movimenti laterali e ricognizioni interne, con generazione automatica di alert ad alta priorità mappati su MITRE ATT&CK; il deployment di tecnologie deceptive è subordinato all'accordo esplicito dell'Ente interessato, che ne deve condividere l'attivazione in quanto comporta l'installazione di sistemi presso la propria infrastruttura e attività che vanno oltre il mero monitoraggio passivo; l'adesione è volontaria per ciascun Ente e formalizzata tramite apposito accordo operativo;

**Metrica di dimensionamento**

La metrica di dimensionamento è a canone annuale.

### 3.1.4 Cyber Threat Intelligence (CTI) e MISP Regionale

Il servizio di CTI dovrà evolvere da un approccio puramente descrittivo a una leva operativa a supporto del SOC.

**REQUISITI DA ATTUARE ALL'AVVIO DEL SERVIZIO**

**Gestione della MISP Regionale**

- mantenimento e gestione della MISP Regionale (Malware Information Sharing Platform), interconnessa con il CSIRT Italia, quale punto di accentramento degli Indicatori di Compromissione per l'intera constituency;
- applicazione del protocollo TLP (Traffic Light Protocol) per la classificazione e la condivisione sicura delle informazioni di intelligence;
- garanzia che tutti gli IoC e le informazioni di intelligence strutturate siano scambiati in formato STIX 2.1 tramite TAXII 2.1; non è ammesso il ricorso a formati proprietari;
- aggiornamento con cadenza almeno annuale dei perimetri tecnologici degli Enti connessi alla MISP;
- iscrizione obbligatoria ai programmi di info-sharing promossi da ACN ai sensi dell'art. 17 del D.Lgs. 138/2024 (NIS2), con particolare riferimento alla piattaforma MISP ACN; l'iscrizione deve essere completata entro 30 giorni dall'avvio del servizio e mantenuta attiva per tutta la durata contrattuale;
- fornitura periodica ad ACN di dati aggregati sugli eventi di sicurezza monitorati nella Constituency, in linea con la tassonomia TC-ACN e nel rispetto delle indicazioni operative di ACN per fini statistici e di reportistica nazionale; i dati trasmessi devono essere anonimizzati e non devono consentire l'identificazione dei singoli Enti salvo consenso esplicito;

**Feed e integrazione operativa**

- acquisizione e integrazione delle seguenti fonti come feed obbligatori minimi attivi sin dall'avvio del servizio:
    - CERT-AGID IoC — fonte nazionale obbligatoria per gli indicatori di compromissione relativi alle minacce che colpiscono la PA italiana;
    - MISP ACN — piattaforma nazionale di info-sharing dell'Agenzia per la Cybersicurezza Nazionale, come previsto dall'obbligo di iscrizione ai sensi dell'art. 17 D.Lgs. 138/2024;
    - National Vulnerability Database (NVD) — feed di vulnerability intelligence in formato JSON e RSS per il monitoraggio continuo delle vulnerabilità note (CVE); il feed deve essere integrato con il CMDB degli Enti per la prioritizzazione contestuale degli alert;
    - almeno una fonte di indicatori aggregati tra SANS Internet Storm Center, OSVDB o equivalente documentato con metodologia pubblica;
- acquisizione e messa a disposizione di flussi strutturati di Indicatori di Compromissione (IoC), comprensivi almeno di: domini sospetti, hash di malware noti, indirizzi IP associati ad attività dannose, URL contenenti codice malevolo, e monitoraggio dei principali siti di condivisione pubblica (es. Pastebin e equivalenti) per il rilevamento di credential leak e codice malevolo condiviso; tale copertura è obbligatoria sin dall'avvio del servizio e non soggetta a maturazione progressiva;
- esposizione di API di integrazione documentate e accessibili al CERT regionale e agli Enti della Constituency per l'automazione della raccolta e distribuzione delle informazioni di intelligence; le API devono consentire almeno: interrogazione degli IoC attivi per ente o per categoria, recupero automatizzato dei bollettini di threat intelligence, e integrazione con i sistemi SIEM/SOAR degli Enti che lo richiedono; la documentazione delle API deve essere consegnata entro 30 giorni dall'avvio del servizio;
- erogazione di segnalazioni CTI puntuali e contestualizzate verso i singoli Enti, con meccanismo di push automatico degli alert di Threat Intelligence e prioritizzazione basata sul settore di appartenenza, sulle tecnologie in uso e sulle vulnerabilità note presenti nel CMDB di ciascun Ente;
- arricchimento automatico degli alert SOC con il contesto di Threat Intelligence disponibile, includendo per ciascun alert: fonte dell'IoC, livello di confidenza, data di prima rilevazione, campagne associate note e indicazioni di mitigazione;
- utilizzo degli SBOM forniti dal servizio di Vulnerability Management come strumento di contestualizzazione e prioritizzazione delle segnalazioni CTI, con correlazione automatica tra CVE nuove e asset effettivamente esposti nella Constituency;

**REQUISITI DA ATTUARE ENTRO I TERMINI INDICATI**

- **entro 6 mesi** — raccolta, analisi e contestualizzazione delle minacce provenienti dal Deep Web e Dark Web, con copertura esplicita di fenomeni quali data leakage, credential leakage e domain squatting riferiti specificamente agli Enti della Constituency e ai loro domini istituzionali; il monitoraggio dei siti di condivisione pubblica (Pastebin e equivalenti) è invece obbligatorio sin dall'avvio come previsto nei requisiti minimi;
- **entro 6 mesi** — acquisizione e integrazione di feed TI settoriali: ISAC di settore rilevanti per la constituency (sanità, Pubblica Amministrazione), con SLA di aggiornamento documentato;
- **entro 12 mesi** — ampliamento progressivo della platea degli Enti connessi alla MISP Regionale, con supporto attivo nel processo di integrazione con i propri apparati di sicurezza;
- **entro 12 mesi** - interconnessione della MISP Regionale con la Polizia Postale, in aggiunta alla connessione obbligatoria con il CSIRT Italia;
- **entro 6 mesi** - feed TI commerciali aggiuntivi con SLA di aggiornamento inferiore alle 4 ore per gli IoC critici;

**Metrica di dimensionamento e modalità di remunerazione CTI**

Il servizio di Cyber Threat Intelligence è remunerato tramite canone annuale articolato in due componenti:

Componente fissa pari all'80% — copre il mantenimento dei feed obbligatori minimi (CERT-AGID, MISP ACN, NVD e almeno una fonte aggregata), la gestione della MISP Regionale, l'erogazione delle API di integrazione e le attività operative di contestualizzazione e distribuzione degli alert CTI verso gli Enti. La componente fissa è indipendente dai risultati conseguiti sugli obiettivi di cui alla componente variabile ed è dovuta per l'intera durata contrattuale.

Componente variabile pari al 20% — riconosciuta in funzione del grado di raggiungimento degli obiettivi annuali di sviluppo del servizio, articolati nelle tre componenti di seguito indicate:

| Componente | Quota sul canone | Indicatore |
|---|---|---|
| Produzione di intelligence | 8% | Numero di eventi qualificati pubblicati sulla MISP Regionale nell'anno |
| Diffusione presso la Constituency | 7% | Numero di Enti connessi e operativi sulla MISP Regionale al termine dell'anno |
| Utilità operativa | 5% | Numero di alert CTI contestualizzati distribuiti agli Enti nell'anno |

**Definizione di evento qualificato.** Ai fini del primo indicatore si computano esclusivamente gli eventi che soddisfano congiuntamente tutte le seguenti condizioni, verificabili come attributi della piattaforma MISP:

- evento creato dall'organizzazione dell'Aggiudicatario, come risultante dal relativo identificativo di organizzazione;
- evento pubblicato e distribuito agli Enti della Constituency;
- evento classificato secondo il protocollo Traffic Light Protocol;
- evento associato ad almeno un cluster di contestualizzazione della minaccia, con riferimento a tecniche MITRE ATT&CK, gruppi di attaccanti o campagne;
- evento corredato di descrizione e di indicazioni operative di rimedio.

Gli eventi importati da fonti esterne, ancorché presenti sulla piattaforma, non concorrono al computo.

**Definizione di Ente connesso e operativo.** Ai fini del secondo indicatore si computano gli Enti che dispongano di un'utenza attiva sulla MISP Regionale e che abbiano effettuato almeno un accesso o ricevuto almeno una distribuzione nell'ultimo trimestre dell'anno di riferimento.

**Modalità di calcolo.** Per ciascuna delle tre componenti si determina il rapporto tra il risultato conseguito e il corrispondente obiettivo annuale. La quota è riconosciuta secondo il seguente criterio:

- rapporto inferiore al 50%: nessuna erogazione della quota;
- rapporto compreso tra il 50% e il 100%: erogazione della quota in misura proporzionale al rapporto conseguito;
- rapporto pari o superiore al 100%: erogazione dell'intera quota, senza riconoscimento di importi ulteriori.

Le tre componenti sono valutate autonomamente: il mancato raggiungimento dell'obiettivo di una componente non incide sull'erogazione delle altre.

**Obiettivi del primo anno contrattuale.** Tenuto conto dello stato di utilizzo della piattaforma alla data di avvio del servizio, gli obiettivi del primo anno sono i seguenti:

| **Indicatore** | **Obiettivo primo anno** |
|---|---|
| Eventi qualificati pubblicati sulla MISP Regionale | 60 |
| Enti connessi e operativi sulla MISP Regionale | 10 |

| | |
|---|---|
| Alert CTI contestualizzati distribuiti agli Enti | 500 |

**Revisione annuale degli obiettivi.** Gli obiettivi relativi a ciascun anno contrattuale successivo al primo sono determinati dalla Stazione Appaltante, sentito l'Aggiudicatario, in sede di Stato Avanzamento Attività, entro sessanta giorni antecedenti l'inizio dell'anno di riferimento, sulla base dei risultati conseguiti nell'anno precedente, dell'evoluzione della Constituency e del contesto di minaccia. In difetto di determinazione entro il termine indicato si intendono confermati gli obiettivi dell'anno precedente.

**Verifica e rendicontazione.** I valori dei tre indicatori sono estratti dalla piattaforma MISP Regionale e dai sistemi di distribuzione degli alert, rendicontati con cadenza mensile nel report di Stato Avanzamento Attività e consolidati a consuntivo annuale. La Stazione Appaltante può richiedere in qualsiasi momento l'esportazione dei dati elementari a supporto della rendicontazione.

Il numero minimo di feed attivi garantiti è dichiarato dall'Aggiudicatario in offerta tecnica e non può essere inferiore a 5, di cui 4 obbligatori come indicato ai requisiti minimi del presente articolo (CERT-AGID, MISP ACN, NVD e almeno una fonte di indicatori aggregati tra SANS Internet Storm Center, OSVDB o equivalente documentato). La riduzione del numero di feed attivi al di sotto del minimo dichiarato in offerta costituisce inadempimento soggetto alle penali previste nell'Allegato C1 - Indicatori di qualità.

### 3.1.5 Reperibilità, Crisis Management e SLA inderogabili

L'Aggiudicatario dovrà garantire un servizio di pronta reperibilità H24x7x365 per l'eventuale supporto al servizio di reperibilità e governance (§2.1.5) nel casi di crisi derivanti da incidenti ad impatto critico — quali attacchi ransomware, indisponibilità di servizi essenziali ed esfiltrazione di dati — occorsi agli Enti della Constituency.

**Gestione della crisi**

Partecipazione alla War Room dedicata (§2.1.5). il Service Manager di cui al §3.1.1, quale punto di riferimento contrattuale unico del Servizio, partecipa alla War Room in caso di incidenti di Severità 1 (S1) e ha la responsabilità di coadiuvare la governance regionale sull'evoluzione della crisi,

**Processo strutturato di Incident Response**

Il processo di Incident Response si articola obbligatoriamente nelle seguenti fasi, ciascuna con i propri deliverable:

- Segnalazione: il fornitore è tenuto a segnalare tempestivamente alla stazione appaltante e all'Ente interessato qualsiasi incidente rilevato o di cui sia venuto a conoscenza, sia che interessi direttamente i sistemi dell'Ente, sia che origini nei sistemi del fornitore stesso o nella sua catena di fornitura e possa avere impatti sulla sicurezza, disponibilità o integrità dei servizi erogati;

- Identificazione e analisi: Avviso di preallarme: prima investigazione dell'incidente, con indicazione se la segnalazione sia riconducibile a un incidente reale o a un falso positivo; deve essere trasmesso al referente tecnico dell'Ente entro i tempi SLA previsti nell'Allegato C1 - Indicatori di qualità per ciascun livello di severità;
- Raccolta delle evidenze: acquisizione delle evidenze digitali in modalità forense nei casi in cui si preveda un prosieguo in ambito legale, con trasmissione al referente tecnico dell'Ente e archiviazione sicura;

Le attività di remediation e ripristino sono in carico all'ente partecipante alla Constituency. Il fornitore deve utilizzare il sistema di trouble ticketing adottato dalla governance per la tracciabilità completa di tutte le fasi del processo.

### 3.1.6 Medical SOC (requisiti specifici per la sanità)

Il servizio di Medical SOC è erogato in forma sperimentale a favore di almeno una singola Azienda Sanitaria della Constituency, individuata dalla stazione appaltante. La sperimentazione costituisce un obbligo contrattuale a tutti gli effetti, incluso nel perimetro del presente servizio.

Qualora nel corso della durata contrattuale dovessero rendersi disponibili ulteriori risorse economiche, la stazione appaltante si riserva la facoltà di estendere il servizio ad altre Aziende Sanitarie della Constituency, fino a coprire l'intera platea delle aziende sanitarie e socio-sanitarie, mediante apposito atto aggiuntivo. L'Aggiudicatario si impegna sin d'ora a garantire la propria disponibilità all'estensione del servizio alle medesime condizioni tecniche ed economiche offerte in sede di gara.

Il servizio dovrà essere focalizzato sulla protezione delle reti cliniche e dei dispositivi medici connessi, con particolare riguardo all'ecosistema IoMT (Internet of Medical Things). Il contesto sanitario pone vincoli specifici che non si riscontrano negli altri modelli architetturali: i dispositivi medici sono frequentemente soggetti a certificazioni di prodotto che ne impediscono l'aggiornamento autonomo, operano su sistemi operativi non più supportati e non possono essere gestiti con le tecniche di hardening tradizionali senza invalidare le garanzie contrattuali del fornitore. Il servizio dovrà tenere conto di questi vincoli strutturali in ogni fase operativa.

Il censimento iniziale dei dispositivi IoMT di cui al presente articolo è soggetto alla milestone M17 (§3.1.2), con termine di 90 giorni dalla data di individuazione dell'Ente sanitario pilota da parte della stazione appaltante.

Requisiti minimi obbligatori

**Inventario e visibilità degli asset clinici**

- censimento passivo dei dispositivi IoMT connessi alla rete clinica mediante osservazione del traffico di rete e telemetria NDR, senza installazione di agent o software intrusivi sugli apparati; l'approccio passivo è inderogabile per preservare la validità delle certificazioni dei dispositivi e la continuità assistenziale;
- mantenimento di un inventario aggiornato degli asset clinici, integrato con il CMDB dell'Ente sanitario, con classificazione dei dispositivi per criticità clinica, stato di aggiornamento del firmware e livello di esposizione al rischio;

- aggiornamento periodico dell'inventario con cadenza almeno trimestrale, o a seguito di variazioni significative nell'infrastruttura di rete clinica;

**Guardrail clinici e gestione della risposta**

- definizione e applicazione di guardrail clinici vincolanti: qualsiasi azione di contenimento automatizzata (SOAR) su asset classificati come safety-critical — quali monitor di parametri vitali, pompe di infusione, sistemi di sala operatoria e apparecchiature diagnostiche — deve essere soggetta a un processo di approvazione esplicita da parte del responsabile clinico o tecnico dell'Ente, prima dell'esecuzione;
- sviluppo di Playbook specifici per gli scenari di attacco più rilevanti in ambito sanitario — tra cui ransomware su sistemi di cartella clinica elettronica, compromissione di sistemi PACS/RIS e accessi non autorizzati a reti cliniche segmentate;
- in nessun caso le azioni automatizzate di risposta potranno determinare l'interruzione di dispositivi o sistemi direttamente coinvolti nell'erogazione di cure al paziente, salvo esplicita autorizzazione scritta della direzione sanitaria dell'Ente;

**Controllo della supply chain clinica**

- monitoraggio degli accessi remoti dei fornitori di dispositivi medici e software clinico, tramite session logging completo, autenticazione a più fattori (MFA) e rispetto di finestre manutentive preventivamente autorizzate dall'Ente;
- segnalazione immediata al SOC di qualsiasi accesso remoto avvenuto al di fuori delle finestre autorizzate o con credenziali non attese, con apertura automatica di un ticket di sicurezza;
- produzione di un report trimestrale sugli accessi remoti dei fornitori, con evidenza delle sessioni effettuate, durata, sistemi coinvolti ed eventuali anomalie rilevate;

Requisiti a maturazione progressiva

- entro 12 mesi — sviluppo e mantenimento di regole di detection specifiche per il traffico generato da dispositivi IoMT, inclusi protocolli clinici (HL7, DICOM, FHIR) e protocolli industriali eventualmente presenti nelle reti ospedaliere;
- entro 12 mesi — mappatura delle anomalie rilevate alle tattiche e tecniche MITRE ATT&CK for ICS e MITRE ATT&CK for Enterprise, con distinzione tra asset IT e asset OT/IoMT nel report di coverage mensile;
- entro 12 mesi — integrazione nel processo di monitoraggio clinico degli SBOM dei dispositivi IoMT, forniti dal servizio di Vulnerability Management ove disponibili; il SOC dovrà segnalare al servizio VM le lacune informative rilevate per gli asset privi di SBOM;
- entro 12 mesi — monitoraggio delle vulnerabilità note sui dispositivi medici con riferimento ai bollettini dei produttori, alle segnalazioni ENISA e agli avvisi del CERT-

AGID e del CSIRT Italia; a parità di score CVSS, un dispositivo con componente vulnerabile identificato nello SBOM e privo di aggiornamento autorizzato dal produttore dovrà essere classificato ad alto rischio;

Elementi premiali

- utilizzo della nomenclatura EMDN (European Medical Device Nomenclature) come sistema di classificazione di riferimento per la categorizzazione dei dispositivi IoMT nell'inventario; la percentuale di dispositivi classificati con codice EMDN è riportata mensilmente come indicatore di miglioramento continuo;
- disponibilità a estendere il servizio ad altre Aziende Sanitarie della Constituency al medesimo prezzo unitario offerto in sede di gara, qualora si rendessero disponibili finanziamenti aggiuntivi.

## 3.2 Vulnerability Management

### 3.2.1 Oggetto del servizio e vincoli metodologici (gestione forte)

Il Servizio ha per oggetto i servizi proattivi di Vulnerability & Exposure Management, Penetration Testing, Purple Teaming e di seguito descritti, erogati attraverso un modello di "gestione forte" e centralizzata.

### 3.2.2 Vulnerability & Exposure Management "assistito"

Il servizio dovrà evolvere da un approccio puramente "CVE-centrico" a un vero e proprio "Exposure Management", in cui le priorità sono stabilite in base al contesto, all'esposizione su internet, alla criticità del servizio e all'effettiva sfruttabilità (exploitability) della vulnerabilità individuata. servizio dovrà prevedere un cruscotto di gestione che riporti lo stato delle rilevazioni nel loro percorso (segnalazione e remediation). L'Aggiudicatario dovrà inoltre garantire:

- **centralizzazione delle evidenze:** raccogliere e integrare le vulnerabilità provenienti da *tutti* i servizi dell'ecosistema di sicurezza ( SOC, VA/PT, Cyber Threat Intelligence e audit tecnici) al fine di ottenere una vista centralizzata e coerente del rischio tecnologico generale;

- **modello a fasi interdipendenti (End-to-End):** non limitarsi alla consegna di report di scansione, ma realizzare un monitoraggio e controllo dalla rilevazione alla "remediation", capitalizzando pienamente i risultati dei test;

- **vulnerability management assistito:** integrare fortemente il processo con il SOC e supportare proattivamente gli Enti nell'identificazione, prioritizzazione e gestione operativa per la chiusura delle vulnerabilità critiche.

### 3.2.3 Attività di Vulnerability Assessment

Nell'ambito del presente servizio, l'Aggiudicatario dovrà erogare attività di **Vulnerability Assessment (VA)** su un perimetro complessivo fino a **13.000 indirizzi IP per anno**, distribuiti sull'infrastruttura degli Enti aderenti al Servizio. Le attività di VA dovranno rispettare i seguenti requisiti minimi:

- **perimetro e pianificazione:** il piano annuale di assessment dovrà coprire l'intero parco di asset concordato, con un approccio di scansione sia **authenticated** che **unauthenticated**, adattato alla tipologia e alla criticità degli asset (server, endpoint, dispositivi di rete, sistemi OT/IoT medicali ove applicabile);
- **frequenza e continuità:** le scansioni dovranno essere condotte con frequenza **almeno semestrale** per gli asset classificati ad alta criticità e **almeno annuale** per gli asset a criticità medio-bassa, garantendo comunque una copertura continuativa e la rilevazione tempestiva di nuove esposizioni;
- **strumentazione e metodologia:** l'Aggiudicatario dovrà impiegare piattaforme di VA di livello enterprise (es. Tenable, Qualys, Rapid7 o equivalenti), integrate nell'ecosistema di Exposure Management, assicurando l'aggiornamento continuo dei

plugin/signature e l'adozione delle principali metodologie di riferimento (OWASP, NIST SP 800-115, PTES);

- **prioritizzazione contestuale:** i risultati delle scansioni non dovranno essere consegnati come meri elenchi di CVE, bensì dovranno essere **arricchiti e contestualizzati** mediante correlazione con feed di Cyber Threat Intelligence, indicatori di exploitability attiva (es. EPSS, CISA KEV) e informazioni sull'esposizione internet degli asset, al fine di produrre una graduatoria di rischio effettivo e azionabile;
- **reportistica e deliverable:** al termine di ogni ciclo di scansione dovrà essere prodotto un **report tecnico** per gli amministratori di sistema e un **report esecutivo** per il management dell'Ente, contenente almeno: riepilogo delle vulnerabilità rilevate per severità (Critical/High/Medium/Low), trend rispetto al ciclo precedente, top-10 vulnerabilità prioritarie con indicazione del piano di remediation suggerito e relativi tempi stimati;
- **tracciamento della remediation:** le vulnerabilità rilevate dovranno essere tracciate all'interno della piattaforma centralizzata di Exposure Management, con indicazione dello stato (aperta, in lavorazione, risolta, accettata), del responsabile e delle scadenze concordate, consentendo la verifica puntuale della chiusura attraverso scansioni di **re-test** mirate;
- **integrazione con il SOC:** le vulnerabilità critiche e ad alta priorità dovranno essere automaticamente notificate al SOC per la correlazione con gli alert di sicurezza in corso, abilitando una risposta coordinata e riducendo i tempi di esposizione a rischio concreto.

### 3.2.4 - Monitoraggio Continuo della Superficie di Attacco Esterna (EASM) e Shadow IT

Al fine di colmare il divario temporale insito nelle scansioni periodiche di Vulnerability Assessment (VA) e di identificare proattivamente le esposizioni accidentali prima che vengano sfruttate da attori malevoli, l'Aggiudicatario dovrà implementare e gestire un servizio di External Attack Surface Management (EASM).

Il servizio dovrà operare in modalità continua e automatizzata, garantendo l'aggiornamento della postura di sicurezza esterna con frequenza almeno giornaliera. L'EASM non dovrà limitarsi all'analisi degli asset statici forniti dagli Enti (inventario noto), ma dovrà svolgere un'attività di *Discovery* autonoma per l'individuazione del cosiddetto "Shadow IT" e degli asset non censiti (es. sottodomini orfani, ambienti di staging/test dimenticati, server cloud o repository di codice accidentalmente esposti al pubblico, domini simili utilizzati per campagne di typo-squatting).

Il servizio EASM dovrà obbligatoriamente garantire le seguenti funzionalità e integrazioni minime:

- **Rilevamento delle criticità "Zero-Day" ed esposizioni fatali:** Identificazione immediata di interfacce di amministrazione esposte in modo non sicuro (es. RDP, SSH, Telnet, pannelli di login di firewall/VPN senza MFA), bucket di storage cloud pubblici e vulnerabilità critiche di recente pubblicazione (es. CISA KEV) sfruttabili senza autenticazione della rete internet.
- **Integrazione operativa End-to-End con il SOC:** Qualsiasi esposizione classificata come critica o ad alto rischio (es. database non protetto, porta gestionale esposta) rilevata

dall'EASM dovrà generare automaticamente e in tempo reale un alert di sicurezza all'interno del sistema di ticketing del SOC Regionale, bypassando le normali tempistiche di reportistica del Vulnerability Management.

- **Alimentazione dinamica dell'inventario:** Le evidenze raccolte e validate dall'EASM dovranno alimentare e aggiornare automaticamente il CMDB (Configuration Management Database) di ciascun Ente, correlando gli asset scoperti con gli SBOM disponibili e i dati di Threat Intelligence (CTI).
- **Reportistica dedicata:** Fornitura di un cruscotto (dashboard) e di un report mensile che evidenzi le fluttuazioni della superficie di attacco per ciascun Ente (es. "nuovi asset esposti nel mese", "servizi deprecati ancora visibili"), dimostrando la progressiva riduzione e messa in sicurezza del perimetro esterno.

### 3.2.4 Penetration test e purple teaming

Per testare la resilienza delle infrastrutture ICT e l'efficacia dei sistemi di difesa della Constituency, l'Aggiudicatario dovrà eseguire test di sicurezza avanzati, andando oltre le attività canoniche:

- **Penetration Test (PT):** esecuzione di test di penetrazione mirati su servizi critici, infrastrutture a seguito di modifiche rilevanti (change management) e su qualsiasi tipologia di applicazione (inclusi sistemi web, backend, API e applicazioni mobile), al fine di validare catene di attacco realistiche e verificare l'efficacia delle contromisure di sicurezza. L'Aggiudicatario dovrà garantire l'esecuzione di test fino a complessive 100 applicazioni all'anno, indipendentemente da dimensioni e tipologia, incluse applicazioni per dispositivi mobili, in conformità con le priorità stabilite dagli Enti e con l'evoluzione del rischio cyber.

- **Purple Teaming:** l'Aggiudicatario dovrà arricchire il processo di verifica integrando esercitazioni di "Purple Teaming" - tali esercitazioni dovranno combinare le competenze offensive (Red Team) e difensive (Blue Team) con l'obiettivo di testare in modo realistico ed evoluto le capacità di *detection, response* e coordinamento del SOC dello CSIRT e dei team di sicurezza degli Enti.

### 3.2.5 Secure coding / DevSecOps e supply chain software

L'Aggiudicatario dovrà definire il perimetro e i requisiti di sicurezza per la supply chain del software, agendo come guida metodologica e di controllo per l'Ente. In particolare:

- **requisitazione per Uffici Acquisti:** definire una rigorosa requisitazione tecnica da condividere con gli Uffici Acquisti degli Enti per assicurare che gli approvvigionamenti rispettino le normative vigenti in materia di sviluppo sicuro del codice, utilizzo consapevole dell'Intelligenza Artificiale (IA) e del Cloud;

- **governance DevSecOps e SBOM:** introdurre policy per la valutazione del rischio derivante dalle dipendenze open source (Software Composition Analysis - SCA),

gestione dei segreti (token/chiavi) e adozione della SBOM (Software Bill of Materials) per i progetti critici

### 3.2.6 Gestione degli SBOM (Software Bill Of Materials)

A supporto del processo di Vulnerability Management, l'Aggiudicatario dovrà promuovere e gestire la raccolta degli SBOM (Software Bill of Materials) dei sistemi e dei componenti software rilevanti per la sicurezza degli Enti della Constituency. La gestione degli SBOM costituisce un requisito abilitante per la correlazione puntuale tra vulnerabilità note e asset effettivamente esposti, in linea con quanto previsto dal Regolamento UE Cyber Resilience Act (CRA), la cui applicazione progressiva interessa l'intera durata contrattuale.

**Acquisizione e mantenimento degli SBOM**

L'Aggiudicatario dovrà acquisire, mantenere e integrare nel CMDB gli SBOM dei sistemi e delle applicazioni rilevanti per la sicurezza, ove resi disponibili dai produttori o dalle fonti pubbliche. Nel dettaglio:

- gli SBOM saranno acquisiti da fonti primarie (produttori software) o da repository pubblici accreditati, quali NVD e CISA;
- gli SBOM dovranno essere mantenuti aggiornati e integrati nel CMDB, con cadenza almeno trimestrale e in formato strutturato aperto (CycloneDX o SPDX);
- l'Aggiudicatario dovrà supportare gli Enti nella richiesta degli SBOM ai propri fornitori software, in conformità con quanto previsto dal Regolamento UE Cyber Resilience Act (CRA);
- gli SBOM dovranno essere resi disponibili al SOC tramite integrazione con il CMDB, in tempo utile per la correlazione operativa.

**Utilizzo degli SBOM nel processo di Vulnerability Management e CTI**

Gli SBOM costituiscono lo strumento primario di correlazione tra le vulnerabilità note (CVE) e gli asset effettivamente esposti. L'Aggiudicatario dovrà garantire che:

- gli SBOM siano utilizzati come strumento primario di correlazione tra le vulnerabilità note (CVE) e gli asset effettivamente esposti, consentendo al SOC di rispondere con precisione e tempestività all'emergere di nuove minacce;
- quando vengono identificate vulnerabilità attivamente sfruttate o nuovi IoC associati a componenti software specifici, la CTI interroghi gli SBOM disponibili degli Enti per determinare quali siano effettivamente esposti e produca segnalazioni mirate esclusivamente nei loro confronti, evitando comunicazioni non pertinenti e aumentando il valore operativo di ogni alert distribuito;
- le lacune informative per gli asset privi di SBOM siano documentate e segnalate agli Enti interessati come fattore di rischio residuo, con aggiornamento nel registro delle lacune allegato al CMDB.

**Gestione degli SBOM per dispositivi IoMT**

Con specifico riferimento agli Enti del comparto sanitario, l'Aggiudicatario dovrà curare la raccolta e la gestione degli SBOM relativi ai dispositivi IoMT (Internet of Medical Things). In particolare:

- gli SBOM dei dispositivi IoMT saranno raccolti ove resi disponibili dai produttori, al fine di consentire la correlazione immediata tra vulnerabilità note (CVE) e componenti software presenti nell'inventario clinico;
- l'Aggiudicatario dovrà supportare le Aziende Sanitarie nella richiesta degli SBOM ai produttori dei dispositivi medici, anche avvalendosi dei canali istituzionali previsti dal Cyber Resilience Act, e nella loro integrazione nel processo di Vulnerability Management;
- in assenza di SBOM forniti dal produttore, dovrà essere documentata e segnalata all'Ente la relativa lacuna informativa come fattore di rischio, con indicazione del dispositivo coinvolto e della tipologia di componenti non documentati.

### 3.2.7 Dimensionamento del servizio

La metrica di dimensionamento del servizio è a canone annuale.

## 3.3 Gestione del Rischio, TPRM e Business Continuity

### 3.3.1 Gestione del rischio

Il servizio si articola in un processo End-to-End finalizzato a supportare gli Enti della Constituency nell'identificazione, analisi, valutazione, trattamento e monitoraggio continuo dei rischi di cybersicurezza, secondo un approccio progressivo e proporzionato alla dimensione, alla tipologia, al livello di maturità e alla criticità dei servizi erogati da ciascun Ente.

L'esecuzione delle attività dovrà avvenire in coerenza con il framework metodologico definito nell'ambito del servizio e in conformità ai principali standard e riferimenti nazionali e internazionali in materia di risk management e cybersecurity, tra cui, a titolo esemplificativo e non esaustivo, ISO/IEC 27005, ISO 31000, NIST Cybersecurity Framework, NIST SP 800-30 ed ENISA.

L'Aggiudicatario dovrà garantire che il processo di gestione del rischio non si limiti a rilevazioni documentali occasionali, ma si configuri come un presidio continuativo, integrato con gli altri servizi del presente Capitolato Tecnico e alimentato, ove applicabile, dalle evidenze e dai segnali provenienti dal SOC, dal Vulnerability Management, dalla Cyber Threat Intelligence, dal TPRM, dagli audit, dai test di sicurezza e dagli incidenti eventualmente occorsi.

L'esecuzione del servizio dovrà armonizzarsi con le esigenze operative degli Enti, evitando interferenze con la loro ordinaria attività istituzionale. A tal fine, l'Aggiudicatario dovrà prevedere modalità di raccolta delle informazioni e di conduzione delle attività sufficientemente flessibili da garantire qualità, completezza e affidabilità delle evidenze raccolte.

L'Aggiudicatario dovrà altresì assicurare supporto continuativo agli Enti durante tutte le fasi del processo, mediante assistenza metodologica, affiancamento operativo, chiarimenti interpretativi e supporto nella raccolta e validazione delle informazioni necessarie.

Nell'ambito del servizio, l'Aggiudicatario dovrà garantire almeno le seguenti attività:

- **definizione delle linee guida e del framework metodologico**, mediante predisposizione di una metodologia uniforme per la classificazione, valutazione e trattamento del rischio, comprensiva di criteri di impatto e probabilità, scale di valutazione, criteri di accettazione del rischio e modalità di riesame periodico;

- **esecuzione del maturity assessment e della gap analysis**, con cadenza almeno annuale, al fine di valutare il livello di maturità dell'Ente rispetto ai principali domini della cybersicurezza e individuare gli scostamenti rispetto al livello atteso, definito in accordo con la Stazione Appaltante e con la Governance;

- **esecuzione del risk assessment**, mediante sessioni dedicate con gli Enti, finalizzate all'individuazione dei servizi critici, degli asset a supporto, delle principali dipendenze, delle minacce applicabili, delle vulnerabilità rilevanti e dei potenziali impatti sui processi e sui servizi erogati;

- **analisi e valutazione del rischio**, attraverso la correlazione strutturata tra asset, minacce, vulnerabilità, controlli esistenti e impatti attesi, al fine di determinare il livello di rischio inerente e residuo e definirne la priorità di trattamento;

- **creazione e mantenimento del Risk Register**, inteso quale registro dinamico dei rischi dell'Ente, aggiornato nel tempo e strutturato in modo da associare a ciascun rischio almeno il relativo asset o servizio impattato, il livello di rischio, i controlli esistenti, il responsabile del rischio, le azioni previste e le relative scadenze;

- **definizione e aggiornamento del Piano dei Trattamenti**, mediante supporto agli Enti nell'individuazione e prioritizzazione delle misure correttive, migliorative o compensative più opportune, tenendo conto del rapporto tra rischio, benefici attesi, complessità realizzativa e sostenibilità organizzativa;

- **monitoraggio dell'attuazione delle misure di trattamento**, con verifica periodica dello stato di avanzamento delle azioni concordate, della loro efficacia ai fini della riduzione del rischio e dell'eventuale necessità di aggiornare il profilo di rischio residuo;

- **gestione delle eccezioni e delle accettazioni del rischio**, assicurando che eventuali decisioni di accettazione siano formalizzate, motivate, limitate temporalmente e sottoposte a riesame periodico, con relativa tracciabilità all'interno del Risk Register;

- **produzione della reportistica**, mediante predisposizione di elaborati periodici destinati sia al livello operativo sia al livello direzionale, contenenti almeno lo stato dei rischi principali, l'andamento del piano di trattamento, le criticità aperte, le eventuali accettazioni del rischio e gli elementi utili al monitoraggio della postura di sicurezza dell'Ente.

Per ciascun raggruppamento della Constituency si procederà all'analisi di un numero annuale di servizi non superiore a n, conformemente alla pianificazione definita dalla Stazione Appaltante. La selezione puntuale dei servizi da sottoporre ad analisi sarà soggetta a revisione con cadenza annuale, previo accordo con l'Ente interessato e la supervisione della Governance.

A valle delle attività svolte, l'Aggiudicatario dovrà produrre, per ciascun Ente, almeno i seguenti **deliverable**:

- report di maturity assessment e gap analysis;
- report di risk assessment;
- Risk Register aggiornato;
- Piano dei Trattamenti;
- report periodici di monitoraggio sullo stato dei rischi e delle relative azioni di mitigazione.

Resta inteso che l'implementazione materiale delle misure di trattamento rimane in capo ai singoli Enti, mentre l'Aggiudicatario è responsabile del supporto metodologico, del monitoraggio, della tracciabilità delle attività e della verifica complessiva dell'avanzamento del

processo.

### 3.3.2 Modello evoluto per gli Enti del perimetro NIS2

Per gli Enti rientranti nel perimetro di applicazione del D.Lgs. 138/2024 (recepimento della Direttiva NIS2), il servizio di gestione del rischio dovrà essere erogato secondo un modello evoluto, quale rafforzamento del modello base descritto nei paragrafi precedenti.

Tale modello dovrà essere finalizzato a garantire un livello maggiore di approfondimento, aggiornamento e controllo, in coerenza con gli obblighi normativi applicabili agli Enti essenziali e agli Enti importanti, senza dar luogo a un processo separato rispetto alla gestione ordinaria del rischio.

L'Aggiudicatario dovrà pertanto assicurare che, per gli Enti del perimetro NIS2, il servizio venga svolto con modalità tali da consentire una gestione del rischio maggiormente strutturata, continuativa e documentata, nonché pienamente integrata con gli altri servizi oggetto del presente Capitolato Tecnico.

In particolare, l'Aggiudicatario dovrà garantire:

- **un'analisi del rischio rafforzata**, condotta con un maggiore livello di dettaglio rispetto al modello base, con riferimento ai servizi essenziali o importanti, agli asset e ai processi che li supportano, alle dipendenze tecnologiche e organizzative, nonché ai rischi derivanti da fornitori e soggetti terzi;

- **il raccordo con gli obblighi normativi applicabili,** assicurando che il processo di risk assessment, di valutazione del rischio residuo e di trattamento del rischio consenta di verificare e documentare l'adozione delle misure tecniche, operative e organizzative richieste dal D.Lgs. 138/2024;

- **la predisposizione di una mappatura strutturata delle misure di sicurezza**, atta a correlare, per ciascun Ente, i rischi individuati, i controlli esistenti, le eventuali lacune riscontrate, le azioni di trattamento previste e le misure richieste dal quadro normativo di riferimento;

- **un aggiornamento più frequente del profilo di rischio**, mediante alimentazione continuativa del Risk Register con le evidenze e i segnali provenienti dai servizi SOC, Vulnerability Management, Cyber Threat Intelligence, TPRM, audit, test ed eventuali incidenti, al fine di consentire una rivalutazione tempestiva del rischio e delle relative priorità di intervento;

- **un presidio rafforzato dei rischi di supply chain**, con particolare attenzione ai fornitori ICT, ai servizi cloud, ai software critici, agli accessi remoti di terze parti e, più in generale, a tutti i soggetti esterni che possano avere impatto sulla sicurezza dei servizi essenziali o importanti;

- **una reportistica direzionale dedicata**, finalizzata a rappresentare in modo chiaro e sintetico lo stato di esposizione al rischio dell'Ente, le principali criticità aperte, lo stato

di avanzamento dei piani di trattamento, nonché le eventuali eccezioni o accettazioni del rischio ancora in essere;

- **il supporto alla produzione e all'aggiornamento della documentazion**e, delle evidenze e dei tracciati informativi utili a dimostrare l'effettiva adozione di un modello di gestione del rischio coerente con gli obblighi previsti dalla normativa NIS2.

Resta inteso che, per gli Enti ricompresi nel perimetro NIS2, il servizio non dovrà limitarsi alla sola esecuzione periodica delle attività di assessment, ma dovrà garantire il mantenimento di un presidio continuativo e verificabile nel tempo, orientato al progressivo consolidamento della postura di sicurezza dell'Ente.

L'obiettivo del servizio è pertanto quello di accompagnare gli Enti del perimetro NIS2 verso un modello di gestione del rischio più maturo, strutturato e sostenibile, integrato con la governance della cybersicurezza, con la gestione degli incidenti, con la continuità operativa e con il controllo della catena di fornitura.

### 3.3.3 Third Party Risk Management (TPRM)

Per mitigare in modo strutturato i rischi derivanti dalla catena di fornitura degli Enti, l'Aggiudicatario dovrà implementare un processo di Third Party Risk Management (TPRM) che copra l'intero ciclo di vita del rapporto con le terze parti, dall'onboarding fino alla cessazione del rapporto contrattuale.

L'Aggiudicatario dovrà mettere a disposizione uno strumento dedicato, o funzionalità equivalenti integrate nei tool di governance, per identificare, valutare, monitorare e gestire i rischi connessi a fornitori, partner e soggetti terzi che erogano servizi o trattano dati per conto degli Enti.

Il modello dovrà essere scalabile e commisurato alla criticità del fornitore, al tipo di servizio erogato, al livello di accesso ai sistemi e ai dati, nonché al potenziale impatto che un incidente occorso alla terza parte potrebbe determinare sui servizi dell'Ente.

Tra le attività minime e vincolanti che dovranno essere garantite dall'Aggiudicatario rientrano:

- **censimento e classificazione delle terze parti**, mediante predisposizione e mantenimento di un inventario aggiornato dei fornitori e dei partner rilevanti, classificati in base alla tipologia di servizio erogato, al livello di accesso ai sistemi, alla natura dei dati trattati e alla criticità del rapporto;

- **valutazione del rischio inerente**, basata sulla criticità del servizio reso dalla terza parte, sull'eventuale impatto sulla continuità operativa, sui dati trattati, sull'esposizione tecnologica e sul ruolo del fornitore nella catena di erogazione dei servizi dell'Ente;

- **due diligence proporzionata al livello di rischio**, da svolgere mediante raccolta di evidenze, questionari, documentazione, certificazioni o altre informazioni utili a valutare il livello di affidabilità e maturità della terza parte sotto il profilo della sicurezza;

- **utilizzo del cyber scoring come indicatore di rischio**, ove previsto, esclusivamente quale elemento di supporto alla valutazione e non come unico fattore decisionale, da contestualizzare in relazione ai servizi forniti e all'effettivo impatto sull'Ente;

- **supporto nella gestione delle anomalie e delle criticità riscontrate**, mediante affiancamento agli Enti nell'interlocuzione con i fornitori, nella richiesta di chiarimenti, nella definizione delle azioni correttive e, ove necessario, nella formalizzazione dell'accettazione del rischio residuo;

- **supporto alla definizione di clausole contrattuali di sicurezza**, da inserire nei contratti stipulati dagli Enti con i propri fornitori, con particolare riferimento a obblighi di notifica di incidenti, livelli di servizio, gestione degli accessi remoti, finestre manutentive, protezione dei dati, collaborazione in caso di crisi ed eventuale disponibilità di SBOM e altre evidenze tecniche;

- **monitoraggio continuativo delle terze parti critiche**, mediante aggiornamento periodico della valutazione del rischio e rilevazione di eventuali elementi sopravvenuti che possano incidere sul profilo di rischio del fornitore;

- **gestione degli accessi remoti delle terze parti**, con particolare attenzione agli accessi privilegiati e agli accessi a sistemi critici, assicurando la tracciabilità delle sessioni, l'utilizzo di autenticazione forte e il rispetto delle finestre autorizzate;

- **supporto alla definizione delle exit strategy**, al fine di garantire, al termine del rapporto con il fornitore, la corretta cessazione degli accessi, la restituzione o portabilità dei dati, il trasferimento della documentazione necessaria e la continuità operativa del servizio.

Si riporta di seguito la pianificazione relativa al numero minimo di soggetti terzi da sottoporre a valutazione annuale per ciascun Gruppo:

| Gruppo di appartenenza | n. fornitori per Gruppo |
|---|---|
| **Gruppo 1** | 25 |
| **Gruppo 2** | 15 |
| **Gruppo 3** | 10 |
| **Gruppo 4** | 10 |
| **Gruppo 5** | 5 |

*Tabella 1 – Volumi di valutazione annui per TPRM (Third Party Risk Management)*

La selezione dei fornitori da sottoporre a valutazione sarà effettuata tenendo conto del livello di rischio, della criticità del servizio e delle priorità individuate dall'Ente e dalla Governance.

Per gli Enti rientranti nel perimetro NIS2, il processo di TPRM dovrà essere svolto con un livello di attenzione rafforzato, in coerenza con gli obblighi relativi alla sicurezza della supply chain previsti dalla normativa applicabile.

A valle delle attività svolte, l'Aggiudicatario dovrà produrre almeno i seguenti deliverables:

- inventario e classificazione delle terze parti rilevanti;
- report di valutazione del rischio dei fornitori esaminati;
- evidenze delle due diligence svolte;
- stato delle azioni correttive e delle eventuali eccezioni o accettazioni del rischio;
- report periodico di monitoraggio delle terze parti critiche.

### 3.3.4 Business Continuity & Disaster Recovery (BC/DR): strategia di resilienza avanzata

L'Aggiudicatario dovrà assumere un ruolo proattivo nel rafforzare la resilienza operativa degli Enti, con l'obiettivo di garantire la continuità dei servizi critici e la capacità di ripristino a fronte di eventi avversi, inclusi incidenti cyber ad elevato impatto.

Il servizio dovrà essere erogato secondo un approccio strutturato e progressivo, coerente con le caratteristiche dell'Ente e con il livello di criticità dei servizi erogati, e dovrà coprire in modo integrato le attività di Business Continuity, Disaster Recovery e, ove necessario, di Cyber Recovery.

L'Aggiudicatario dovrà garantire almeno le seguenti attività:

- **esecuzione della Business Impact Analysis (BIA),** finalizzata a identificare i processi e i servizi critici dell'Ente, le relative dipendenze organizzative e tecnologiche, nonché gli impatti derivanti da un'interruzione dei servizi;

- **supporto nella definizione dei parametri di ripristino**, con individuazione e formalizzazione, per ciascun servizio o processo critico, dei valori di **RTO** (Recovery Time Objective), **RPO** (Recovery Point Objective) e, ove applicabile, del periodo massimo tollerabile di interruzione **MTPD**;

- **mappatura delle dipendenze critiche**, includendo infrastrutture, applicazioni, basi dati, servizi cloud, fornitori esterni, personale chiave e ogni ulteriore componente necessaria al corretto funzionamento dei servizi analizzati;

- **redazione, aggiornamento e manutenzione dei piani di Business Continuity e Disaster Recovery,** assicurando che tali documenti siano coerenti con gli esiti della BIA, con i parametri di ripristino definiti e con l'organizzazione dell'Ente;

- **predisposizione dei runbook operativi di ripristino**, per i servizi e i sistemi critici individuati, in modo da consentire l'esecuzione ordinata, verificabile e tempestiva delle attività di recovery;

- **supporto nella definizione delle procedure di crisi**, comprensive di ruoli, responsabilità, escalation, flussi decisionali e modalità di comunicazione interna ed esterna in caso di incidente grave o indisponibilità di servizi critici;

- **supporto nell'esecuzione di test ed esercitazioni periodiche**, sia di tipo direzionale sia di tipo tecnico, finalizzate a verificare l'effettiva applicabilità dei piani, la correttezza delle procedure, la capacità di coordinamento dei soggetti coinvolti e il rispetto dei parametri di ripristino previsti;

- **verifica dei processi di backup e restore**, con particolare riferimento alla capacità di recupero dei dati e dei sistemi critici entro i tempi previsti, nonché alla integrità e disponibilità delle copie di sicurezza;

- **produzione di report post-test e lessons learned,** contenenti l'esito delle prove svolte, gli scostamenti rilevati rispetto agli obiettivi attesi, le criticità emerse e le eventuali azioni correttive da intraprendere;

- **monitoraggio e supporto alla chiusura delle azioni correttive**, derivanti dagli esiti delle esercitazioni, dei test o degli incidenti reali, al fine di garantire un miglioramento continuo del livello di resilienza dell'Ente.

L'avvio del servizio dovrà prevedere momenti di affiancamento e supporto metodologico agli Enti, anche mediante sessioni dedicate e checklist operative, al fine di agevolare la raccolta delle informazioni e la corretta impostazione delle attività di analisi e pianificazione.

Per gli Enti rientranti nel perimetro NIS2, il servizio dovrà essere svolto in coerenza con gli obblighi normativi applicabili in materia di continuità operativa, gestione delle crisi, disaster recovery e disponibilità dei servizi.

A valle delle attività svolte, l'Aggiudicatario dovrà produrre almeno:

- report di Business Impact Analysis;
- definizione dei parametri di ripristino per i servizi analizzati;
- piani di Business Continuity e Disaster Recovery;
- runbook operativi di ripristino;
- report sugli esiti dei test e delle esercitazioni;
- piano delle azioni correttive e relativo stato di avanzamento.

Resta inteso che l'attuazione delle misure tecniche e organizzative previste nei piani, nonché l'implementazione infrastrutturale degli interventi di continuità e ripristino, rimangono in capo ai singoli Enti, mentre l'Aggiudicatario è responsabile del supporto metodologico, della predisposizione documentale, del monitoraggio e della verifica complessiva dell'efficacia del processo.

### 3.3.5 Dimensionamento del servizio

La metrica di dimensionamento del servizio è a canone annuale.

## 3.4 Formazione e Security awareness

### 3.4.1 Oggetto del servizio e piattaforma qualificata ACN

**Descrizione e Obiettivo Strategico del Servizio**

Il Servizio è finalizzato all'erogazione di un programma organico e continuativo di sensibilizzazione e formazione in materia di sicurezza delle informazioni e cybersecurity destinato alla Constituency regionale. L'obiettivo strategico prevede una segmentazione del servizio in due pilastri:

1) Cybersecurity Awareness, destinata all'intera popolazione di circa 80.000 utenti, di cui 67.000 afferenti il modo sanitario, con un impegno formativo compreso tra 8 e 12 ore complessive annuali, finalizzata a consolidare il Fattore Umano (Human Firewall);

2) Formazione per Figure Apicali e Figure Tecniche, dedicata a circa 140 utenti, con un impegno formativo differenziato in base al ruolo: da 9 a 15 ore complessive per le Figure Apicali e da 16 a 20 ore complessive annuali per le Figure Tecniche ed i Referenti per la Cybersecurity, il tutto orientato allo sviluppo di competenze avanzate di gestione del rischio e governance.

L'obiettivo strategico primario è l'evoluzione da un approccio formativo statico a un modello dinamico, continuo, misurabile e altamente personalizzato (role-based). Questa trasformazione mira a consolidare il "Fattore Umano" (Human Firewall), considerandolo l'ultimo e più critico strato di difesa, riducendo drasticamente la probabilità di successo di attacchi che sfruttano tecniche di ingegneria sociale (phishing, vishing, smishing, social engineering).
Il servizio dovrà accrescere la consapevolezza del personale e del management in merito alle principali minacce informatiche e alle relative buone pratiche, contribuendo al rafforzamento del livello complessivo di sicurezza dell'organizzazione e alla tutela efficace dei dati aziendali critici, delle informazioni sensibili e dei dati personali trattati dagli Enti.

La descrizione dell'offerta formativa, comprensiva di metodologie didattiche, articolazione dei moduli, contenuti proposti e modalità di verifica dell'apprendimento, dovrà essere inserita dall'Operatore economico concorrente all'interno della propria proposta e costituirà parte integrante dell'offerta tecnica presentata in sede di gara.

L'Operatore economico concorrente dovrà prevedere e garantire il completamento delle attività di onboarding di tutti gli enti della Constituency entro tre mesi dall'avvio del contratto, al fine di consentire una tempestiva e uniforme erogazione dei percorsi formativi.

**Aree Tematiche e Contenuti Formativi Minimi**

La formazione erogata dovrà coprire, in modo rigoroso e aggiornato, i seguenti ambiti, garantendo la pertinenza con il contesto della Pubblica Amministrazione:

- **Protezione dei Dispositivi:** Linee guida operative e *best practice* per la sicurezza

fisica e logica di *endpoint* e dispositivi mobili (computer portatili, *smartphone* e *tablet*) utilizzati in ambiente lavorativo e in *smart working*.

- **Gestione delle Credenziali:** Rafforzamento della conoscenza sulle metodologie per la creazione di *password* robuste, l'utilizzo di autenticazione a più fattori (MFA) e la corretta protezione delle credenziali d'accesso.

- **Sicurezza delle Informazioni Personali e Aziendali:** Procedure e comportamenti volti alla salvaguardia della riservatezza, integrità e disponibilità delle informazioni, con particolare attenzione alle normative in materia di *Privacy* (GDPR) e alle politiche di sicurezza interne.

- **Riconoscimento e Reazione agli Attacchi:** Identificazione tempestiva dei tentativi di intrusione, frode e truffa veicolati attraverso canali digitali e telefonici (*spam, phishing, social engineering, ecc.*) e le procedure di segnalazione.

- **Quadro Normativo e Governance:** Comprensione e applicazione delle politiche di sicurezza aziendali, dei Piani di Continuità Operativa (BCP) e delle procedure di *Disaster Recovery*.

- **Analisi e Gestione del Rischio:** Elementi fondamentali per la valutazione del rischio, in coerenza con le metodologie e le circolari emesse da Agenzia per l'Italia Digitale (AgID) per la Pubblica Amministrazione.

- **Tecniche di Prevenzione e Risposta agli Eventi:** Illustrazione delle soluzioni di controllo implementate e delle migliori pratiche per la prevenzione e la gestione reattiva degli incidenti di sicurezza (*incident response*).

- **Evoluzione delle minacce basate su Intelligenza Artificiale Generativa:** Il programma didattico dovrà analizzare l'impatto dell'AI generativa nel panorama del cybercrime, con particolare focus su tecniche avanzate di social engineering (come phishing e vishing iper-personalizzati e automatizzati), la creazione di deepfake volti alla disinformazione o alla sostituzione di persona, e lo sviluppo di malware polimorfici. La formazione dovrà fornire al personale gli strumenti concettuali e operativi per riconoscere e mitigare tali attacchi sofisticati.

- **Sicurezza post-quantistica e protezione dei dati:** I moduli dedicati alla crittografia dovranno tenere in debita considerazione l'avvento dei calcolatori quantici e la loro futura capacità di scardinare gli attuali algoritmi di cifratura asimmetrica (es. RSA e ECC). Sarà necessario formare il personale sulla transizione verso la crittografia post-quantistica (PQC), sulle strategie di migrazione dei sistemi della PA e sulla protezione a lungo termine dei dati sensibili e dei segreti di Stato ("harvest now, decrypt later").

In fase di progettazione della nuova offerta formativa nell'ambito Cybersecurity Awareness – rivolta a tutto il personale – l'Operatore economico concorrente terrà in debita considerazione che tra il 2025 e il 2026 è stata erogata formazione e-learning focalizzata sui seguenti argomenti:

Primo percorso formativo (Prima annualità)

Primo modulo - Phishing:
Fornisce strumenti per riconoscere e gestire attacchi di phishing, illustrando le tecniche più comuni utilizzate dai criminali informatici via e-mail, messaggistica e social media.

Secondo modulo - Password:
Tratta le buone pratiche per la gestione sicura delle credenziali, evidenziando il ruolo centrale delle password nella protezione delle risorse digitali.

Terzo modulo - Social Media:
Analizza i rischi legati all'uso dei social network, con focus sulla protezione della privacy e sulla prevenzione di comportamenti che possano compromettere la sicurezza personale e aziendale.

Quarto modulo - Privacy & GDPR:
Introduce i principi fondamentali del Regolamento Europeo sulla protezione dei dati, promuovendo un approccio consapevole e conforme alla normativa da parte di tutti i membri dell'organizzazione.

Quinto modulo - Mobile Device:
Offre indicazioni pratiche per l'uso sicuro di dispositivi mobili e applicazioni, con attenzione alla separazione tra sfera personale e professionale e alla protezione dei dati.

Sesto modulo – Artificial Intelligence:
Fornisce strumenti per riconoscere contenuti falsi o distorti online, evidenziando i rischi di disinformazione e le implicazioni sulla sicurezza informatica.

Settimo modulo - USB Device:
Analizza i rischi legati all'uso di dispositivi USB, in particolare quelli di memorizzazione, e promuove buone pratiche per proteggere i dati da sottrazioni o compromissioni.

Ottavo modulo - E-mail Security:
Offre indicazioni per la gestione sicura della posta elettronica, con focus sulla protezione delle informazioni sensibili e sulla prevenzione di attacchi veicolati via e-mail.

Nono modulo - Malware & Ransomware:
Spiega le principali tipologie di malware, con particolare attenzione al ransomware, e fornisce strategie per ridurre il rischio di infezione e limitare i danni in caso di attacco.

Decimo modulo - Web Browsing:
Fornisce conoscenze pratiche per una navigazione sicura, illustrando i rischi associati all'uso dei browser e dei siti web e le misure di protezione da adottare.

Undicesimo modulo – Deep Fake:
Esamina il fenomeno del deepfake, offrendo strumenti pratici per identificarlo e difendersi dalla disinformazione digitale.

Dodicesimo modulo - Social Engineering:
Approfondisce le tecniche di ingegneria sociale utilizzate dai cyber criminali, evidenziando l'importanza della vigilanza e della protezione delle informazioni personali.

Secondo percorso formativo (Seconda annualità)

Primo modulo - Clean Desk:
Promuove buone pratiche per la protezione delle informazioni sensibili nella postazione di lavoro, con focus su privacy, sicurezza fisica e conformità al GDPR.

Secondo modulo - Smart Working:
Analizza i rischi legati al lavoro da remoto e fornisce strategie per operare in sicurezza fuori dall'ambiente aziendale, proteggendo dati e sistemi.

Terzo modulo - Social Collaboration & Video-Conferencing:
Esamina le minacce associate all'uso di strumenti di collaborazione e videoconferenza, evidenziando l'importanza di un utilizzo consapevole per tutelare privacy e sicurezza.

Quarto modulo - Smishing & Vishing:
Approfondisce le tecniche di phishing via messaggistica e telefonate, sensibilizzando sull'uso prudente di canali considerati erroneamente sicuri.

Quinto modulo - Spear Phishing:
Fornisce strumenti per riconoscere attacchi mirati di phishing, basati sulla raccolta di informazioni personali e professionali per ingannare specifici individui o gruppi.

Sesto modulo - Ransomware:
Esamina la minaccia ransomware, illustrando le conseguenze degli attacchi e le misure preventive per ridurre il rischio e limitare i danni.

Settimo modulo - Multi-Factor Authentication:
Promuove l'adozione di sistemi di autenticazione avanzati e analizza le tecniche con cui gli attaccanti cercano di aggirarli, come Sneaky Phishing e Sim Swap.

Ottavo modulo - IoT Device:
Tratta i rischi legati ai dispositivi interconnessi, sia in ambito personale che professionale, e propone comportamenti sicuri per gestire l'Internet of Things.

Nono modulo - Bluetooth & Wi-Fi:
Fornisce indicazioni per l'uso sicuro delle connessioni wireless, evidenziando i rischi associati alla mobilità e alla connettività continua.

Decimo modulo - Information Classification:
Spiega l'importanza della classificazione delle informazioni per la protezione dei dati, con focus sulle Personal Identifiable Information e sulle pratiche organizzative.

Undicesimo modulo - Data Protection:
Il modulo approfondisce il tema della protezione dei dati con particolare attenzione alla

sicurezza, alla privacy e al rapporto con le normative di qualità e sicurezza delle informazioni, focalizzandosi sul GDPR. È concepito come un aggiornamento avanzato del modulo "Privacy & GDPR", inserito nel percorso di formazione obbligatoria, con contenuti più sofisticati rispetto al primo livello.

Dodicesimo modulo - Social Engineering 2:
Questo modulo riprende il tema del social engineering, illustrando tecniche di attacco basate sull'inganno e sulla manipolazione psicologica. Attraverso esempi concreti, offre ulteriori elementi di consapevolezza sulle strategie utilizzate dai cybercriminali, fungendo da sintesi dei concetti trattati nei moduli del secondo livello.

**Modalità di Erogazione Flessibili e Requisiti Tecnici Aggiuntivi**

Il programma di *awareness* dovrà integrare una pluralità di canali per massimizzare la diffusione e l'efficacia del messaggio, superando la limitazione del solo *e-learning* tradizionale.

- **Formazione Tradizionale e Strutturata:**
    - Corsi frontali in aula (anche virtuale - *webinar*) e moduli di *e-learning* auto-consistenti e tracciabili, strutturati per rilascio progressivo.
- **Formazione Innovativa e Canali Aggiuntivi (*Value Added*):**
    - **Materiale Multimediale/Video Pillole:** Produzione di brevi contenuti video specifici (*micro-learning*) su tematiche critiche (es. configurazione sicura dello *smart working*, gestione di *ransomware*).
    - **Immagini di Sensibilizzazione (*Digital Signage*):** Sviluppo di *visual* impattanti per la distribuzione sui *wallpaper* degli *endpoint* e sugli schermi informativi aziendali.
- **Approcci Esperienziali e Personalizzati:** Utilizzo di metodologie formative basate su **scenari reali** e approcci esperienziali (*gamification, serious game*), diversificati in funzione dell'area organizzativa, del livello gerarchico e della posizione aziendale del discente, garantendo un forte taglio pratico e una totale adeguatezza alla platea dei fruitori.

**Gestione della Documentazione e Attestazioni**

Il materiale didattico prodotto (slide, manuali, *quick reference guides*) dovrà essere fornito in un formato accessibile (**PDF consultabile e scaricabile**), assicurandone la disponibilità permanente per la consultazione successiva. È requisito vincolante il rilascio di **attestati di partecipazione** formalmente validi, gestiti e conservati in un *repository* digitale sicuro sotto la responsabilità dell'Aggiudicatario, per consentirne l'accesso, la verifica e l'audit da parte dell'Ente. L'Aggiudicatario dovrà inoltre garantire il rilascio, la conservazione e la condivisione dei risultati dei questionari di gradimento (Customer Satisfaction) relativi a ogni modulo formativo o simulazione erogata, come ulteriore metrica di valutazione della qualità del servizio.

**Integrazione Tecnica e Gestione del Ciclo di Vita delle Utenze**

- **Autenticazione e Sicurezza dell'Accesso:** Il sistema LMS (Learning Management System) e quello di simulazione dovranno obbligatoriamente supportare l'autenticazione tramite l'**Identity Provider (IdP) degli Enti**, assicurando la piena operatività della funzionalità di **Single Sign-On (SSO)** per tutti gli utenti, facilitando l'accesso e riducendo l'attrito.

- **Mantenimento dell'Accuratezza delle Utenze:** L'allineamento delle anagrafiche degli utenti (inclusi nuovi ingressi, cessazioni e variazioni di dipartimento/ruolo) dovrà essere gestito con una cadenza minima **mensile**, tramite *sync* automatizzati o semi-automatizzati concordati con l'Ente, per garantire la pertinenza dei percorsi formativi assegnati.

- **Riallineamento Nuove Risorse:** I nuovi dipendenti dovranno essere inseriti immediatamente in un percorso formativo *onboarding* intensivo, progettato per portarli al progressivo riallineamento con il livello di *awareness* della popolazione aziendale in un periodo massimo di **12 mesi** dal loro ingresso in servizio.

- **Supporto Tecnico Utenti:** l'Aggiudicatario dovrà garantire un servizio di supporto agli utenti per questioni di accesso e tecniche sulla piattaforma o per chiarimenti sui contenuti formativi, attivo in regime **8x5** (otto ore al giorno, per cinque giorni lavorativi alla settimana) e deve essere garantito anche durante i periodi di ferie tramite l'istituto della turnazione. La gestione del supporto avverrà principalmente attraverso una casella di posta elettronica dedicata, che sarà ospitata sul dominio del CSIRT regionale.

- **Fruibilità:** l'Aggiudicatario dovrà garantire l'accesso da qualsiasi dispositivo (PC, Tablet, Smartphone) e dai più diffusi Browser Internet;

- ***Opzionale (Value Added Service):*** Sarà elemento di valutazione positiva la capacità di gestire in modo nativo il trasferimento di personale tra Enti diversi all'interno della Constituency, garantendo la conservazione dello stato formativo e, in particolare, mantenendo inalterato lo **"zainetto formativo"** (storico completo di tutte le attività svolte comprensivo della documentazione, attestati e dei risultati ottenuti) per assicurare la continuità del percorso di crescita professionale e di *awareness*.

**Vincolo inderogabile ACN (Agenzia per la Cybersicurezza Nazionale)**

Per partecipare è indispensabile che la piattaforma tecnologica proposta dall'Aggiudicatario per l'erogazione dei servizi di e-learning (formazione) e phishing etico (simulazioni) sia qualificata dall'Agenzia per la Cybersicurezza Nazionale (ACN).

Questo requisito è obbligatorio in quanto la soluzione è classificata come servizio cloud (SaaS) destinato all'utilizzo da parte di Enti e Organismi della Pubblica Amministrazione.

### 3.4.2 Formazione continua, segmentata e role-based

**Il Paradigma del *Micro-Learning* Continuo**

L'Aggiudicatario è chiamato a sviluppare e realizzare un piano formativo che abbandoni il paradigma della formazione generica (*"una tantum"* o *check-box*), in favore di un approccio basato su **percorsi di *micro-learning* continui, interattivi e fortemente differenziati nel tempo e nei contenuti**. La formazione deve essere un processo perpetuo, non un evento isolato.

**Segmentazione Avanzata dell'Audience e Design del Percorso Formativo**

Le attività formative vincolanti devono essere basate su una sofisticata analisi dei rischi e delle responsabilità associate a ciascun ruolo. La segmentazione minima richiesta include:

- **Figure Apicali (Dirigenza e Organi di Governo):** Moduli di *formazione executive* specificamente direzionali, concentrati sulla ***governance* del rischio cyber**, l'impatto delle violazioni, gli obblighi di *compliance* (es. *reporting* di incidenti) e la gestione strategica delle decisioni di sicurezza, con un focus sul bilanciamento tra rischio e innovazione.

- **Personale IT e Help Desk Specialistico:** Formazione altamente tecnica e di dettaglio. I contenuti dovranno includere moduli specialistici su procedure avanzate di *incident response*, analisi forense di primo livello, *vulnerability management*, gestione delle minacce persistenti avanzate (APT) e configurazioni di sicurezza specifiche. È richiesta la possibilità di *training hands-on* (laboratori virtuali).

- **Utenti Generici (Impiegati e Personale Amministrativo):** Formazione di base e progressivamente avanzata sulle buone pratiche quotidiane più comuni (gestione sicura delle email, navigazione web, gestione dei dispositivi personali e aziendali, *social network*). Questi percorsi devono essere accessibili, brevi e immediatamente applicabili.

- **Security Champions e Moltiplicatori di Consapevolezza:** Creazione, supporto e gestione di percorsi dedicati alla formazione e al mantenimento di figure chiave all'interno delle aree operative e dipartimentali (i **Security Champions**). Tali figure devono fungere da moltiplicatori di consapevolezza, punto di riferimento interno e *liaison* privilegiato con il team di sicurezza (CSIRT/SOC), potenziando la diffusione capillare della cultura della sicurezza.

**Requisiti Formativi Aggiuntivi**

- **Certificazioni Esterne e Sviluppo di Competenze:** Il perimetro del servizio dovrà prevedere e finanziare la possibilità di erogare o fornire il supporto logistico, organizzativo ed economico finalizzato esclusivamente alla preparazione all'ottenimento di certificazioni esterne professionalizzanti, riconosciute a livello nazionale o internazionale, per il personale tecnico specialistico degli Enti che opera in ambiti di sicurezza critici. Il perimetro del servizio non comprende l'acquisto dei

voucher d'esame, la cui spesa rimarrà a carico dei singoli Enti o dei partecipanti.

- **Referente Cybersecurity (Lg. 90/2024) - Manager Cybersecurity**: L'Aggiudicatario dovrà assicurare il mantenimento e il rinnovo periodico delle certificazioni di Referente Cybersecurity (ai sensi della Legge 90/2024) e di Manager Cybersecurity, ottenute nell'ambito delle attività formative erogate dal CERT regionale nel corso degli anni 2025 e 2026, in conformità allo schema SCH 82 per i professionisti della cybersecurity nelle Pubbliche Amministrazioni e organizzazioni private. Tale impegno include la copertura integrale dei costi di certificazione annuali previsti dall'ente certificatore (ACS Italia). L'Aggiudicatario dovrà inoltre prevedere fino a un massimo di 4 nuove certificazioni di Referente Cybersecurity ogni anno, coprendo anche i relativi costi per l'acquisto dei voucher d'esame.

- **Accreditamento ECM per il Personale Sanitario:** Per l'intera platea del personale afferente agli Enti Sanitari (ASL, Aziende Ospedaliere, etc. - costituenti il Gruppo 1 della Constituency), la piattaforma LMS e l'intero catalogo dei contenuti formativi dovranno possedere l'**accreditamento necessario per consentire il rilascio di Crediti ECM (Educazione Continua in Medicina)**. Questo requisito tecnico-didattico comporta l'integrazione nativa dei requisiti normativi e dei percorsi formativi obbligatori specifici dell'ambito sanitario all'interno del piano formativo cyber. L'aggiudicatario si farà carico anche della progettazione, dell'accreditamento e della rendicontazione dei percorsi formativi ECM in materia di cybersecurity, destinati al personale delle Aziende e degli Enti del Servizio Sanitario e Socio-Sanitario della Regione del Veneto.

### 3.4.3 Campagne interattive di simulazione e phishing etico

Per misurare in maniera oggettiva, concreta e in vivo la resilienza organizzativa e la postura di sicurezza del fattore umano, l'Aggiudicatario dovrà pianificare, personalizzare ed erogare campagne periodiche e a sorpresa di simulazione che replichino fedelmente scenari di attacco realistici (metodologia del Phishing Etico e oltre).

- **Simulazioni Multicanale:** le campagne non si limiteranno al mero invio di e-mail di Phishing simulato, sarà valutata positivamente l'estensione a simulazioni su altri vettori di attacco di ingegneria sociale:
    - *Vishing:* Voice Phishing - simulazione di attacchi telefonici che sfruttano l'inganno vocale;
    - *Smishing:* SMS phishing - attacchi veicolati tramite messaggistica mobile (SMS o piattaforme di messaggistica istantanea.
- **Coerenza e Personalizzazione:** Gli scenari di attacco simulati dovranno essere progettati per essere altamente **coerenti, credibili e contestualizzati** con l'ambiente lavorativo specifico dell'Ente (es. comunicazioni interne urgenti, riferimento a fornitori reali, finte richieste di compliance, normative regionali in vigore). Ove tecnicamente possibile, gli scenari dovranno essere personalizzati per singola unità organizzativa o

dipartimento per massimizzarne il realismo e la difficoltà di rilevazione.

**Gestione Assistita, *Just-in-Time Learning* e Remediation**

- **Feedback e Rinforzo Immediato:** Immediatamente a valle di ciascuna simulazione, l'Aggiudicatario dovrà attivare **moduli formativi di rinforzo immediato (*feedback just-in-time*)**, erogati automaticamente agli utenti che sono risultati "compromessi" (es. hanno cliccato sul link, scaricato un allegato o fornito credenziali). Questi moduli devono spiegare l'errore e fornire il corretto comportamento.

- **Azioni Correttive Mirate:** Dovranno essere previste e implementate **azioni correttive e di *remediation* mirate** e specifiche sessioni formative di recupero (*debriefing* e *remediation*) sui gruppi di utenti, sulle organizzazioni o sugli Enti che i dati di simulazione hanno dimostrato avere i tassi di rischio o di compromissione più elevati e persistenti.

### 3.4.4 Dashboard avanzate, reportistica e miglioramento continuo

Il servizio dovrà garantire la totale trasparenza, tracciabilità e analizzabilità dell'andamento formativo e della postura di sicurezza umana a beneficio dei Referenti per la Sicurezza e del Management.

**Cruscotti di Monitoraggio (*Dashboard*) Interattivi e Granulari**

L'Aggiudicatario fornirà e configurerà una **dashboard di monitoraggio avanzata, personalizzabile e di facile consultazione**.

- La *dashboard* dovrà assicurare una rappresentazione chiara, completa e **granulare** dell'avanzamento dei discenti e dei risultati delle simulazioni.

- Dovrà consentire ai Referenti dell'Ente di segmentare e distinguere agevolmente i risultati e i progressi non solo a livello aggregato, ma anche tra gli uffici centrali, le direzioni specifiche, le strutture territoriali/periferiche e le categorie di ruolo (*role-based*), facilitando l'identificazione immediata delle sacche di rischio.

**Integrazione Dinamica con Dati di Esercizio (*Threat Intelligence*)**

È richiesto un meccanismo evoluto in cui l'Aggiudicatario non si limiti a rendicontare i propri risultati, ma analizzi attivamente le metriche di *awareness* e simulazione integrandole con i **dati reali di *threat intelligence*** e gli *alert* provenienti dal SOC Regionale (gestito nell'ambito del Lotto 2).

- **Ciclo di Miglioramento Continuo:** Questa integrazione ha lo scopo di realizzare un **ciclo virtuoso e continuo di aggiornamento del *training***, adattando e aggiornando tempestivamente i contenuti formativi ai nuovi *pattern* di attacco (*TTP - Tactics, Techniques, and Procedures*) che vengono effettivamente rilevati contro la

Constituency (formazione basata sul rischio reale).

**Reportistica Direzionale (*Executive*) e Azioni Strategiche**

- **Pacchetto Executive Mensile:** Dovrà essere prodotto con cadenza **mensile** un **"Pacchetto Executive"** formale e conciso, destinato specificamente al Top Management e ai Comitati di Direzione.
- Tale report dovrà evidenziare in modo sintetico e di alto livello i principali *trend* di rischio umano, il *benchmarking* delle *performance* tra Enti o direzioni, e proporre in modo **proattivo e motivato le azioni correttive strategiche** raccomandate per la *governance* futura.

### 3.4.5 Dimensionamento del servizio e modalità di remunerazione

La metrica di dimensionamento del servizio “Cybersecurity Awareness” e del servizio “Formazione per Figure Apicali e Figure Tecniche” è: costo annuale utente.

La modalità di remunerazione del servizio di “Security awareness” è: a consumo (utente iscritto al programma).

La modalità di remunerazione del servizio di “Formazione” è: a consumo (proporzionato al numero di ore di formazione effettivamente fruite dall’utente).

# ART 4 - GOVERNO DELLA FORNITURA

Di seguito vengono descritti gli elementi principali che caratterizzano il governo della fornitura richiesta.

## 4.1 Prodotti della fornitura

Nel corso della vigenza contrattuale, i Fornitori di entrambi i lotti dovranno produrre e consegnare deliverable relativi ai diversi servizi/attività gestite, siano essi di pianificazione, di consuntivazione delle attività o risultato di specifiche attività/processi di lavorazione in conformità con gli standard di documentazione dell'Amministrazione, gli standard di qualità definiti nel presente Capitolato e in linea con le migliori pratiche di settore.

Nello specifico i documenti contrattuali che dovranno essere prodotti con le rispettive date di scadenza, sono elencati nella tabella seguente.

| **Prodotto** | **Termine** |
|---|---|
| Piano della Qualità Generale | Entro 30 giorni solari dalla data di sottoscrizione del Contratto e aggiornamento entro 30 giorni dall'avvio del Contratto |
| Piano di Subentro | Entro i primi 15 giorni lavorativi dalla data di sottoscrizione del Contratto |
| Piano di Trasferimento del Know-How | Entro e non oltre i 180 giorni solari antecedenti la data di scadenza del Contratto |
| Rendicontazione attività e risorse mensile (Stato Avanzamento Attività) | Entro il quinto giorno lavorativo del mese successivo a quello di riferimento |
| Rendicontazione attività e risorse trimestrale (Stato Avanzamento Attività) | Entro il quinto giorno lavorativo del mese successivo al trimestre di riferimento del rendiconto |
| Curriculum Vitae delle risorse impiegate | Entro i primi 10 giorni solari dalla data di sottoscrizione del Contratto per le risorse che prenderanno parte alla fase di subentro. Entro 30 giorni dalla scadenza del periodo di subentro per le risorse impiegate all'avvio dell'esecuzione del contratto. |

*Tabella - Prodotti della fornitura*

L'Amministrazione si riserva la facoltà di richiedere ulteriori documenti o di meglio dettagliare i contenuti durante le fasi di avvio delle attività.

Per quanto attiene la documentazione che i Fornitori sono tenuti a presentare, deve garantire caratteristiche qualitative in termini di:

- accuratezza;
- attualità;

- coerenza;
- completezza;
- consistenza.

Per maggiori dettagli su queste caratteristiche si rinvia allo standard internazionale ISO 25024.

## 4.2 Piano della Qualità Generale

Il Piano della Qualità Generale rappresenta lo strumento fondamentale per monitorare e stimare l'efficacia delle prestazioni fornite. Attraverso questo documento si verifica la conformità qualitativa dei servizi lungo tutto il periodo del contratto, prendendo in considerazione le reali necessità manifestate dall'Amministrazione e dagli Enti della Constituency.

Il Piano della Qualità Generale definisce le modalità con cui vengono garantiti il controllo, la misurazione e il miglioramento continuo della qualità dei servizi erogati. Esso assicura l'aderenza agli standard richiesti, specifica i ruoli e le responsabilità coinvolte e disciplina le attività di monitoraggio e verifica della conformità ai requisiti previsti.

Il Piano della Qualità Generale dovrà essere predisposto dai Fornitori di entrambi i lotti e dovrà:

- collegare i requisiti specifici dei servizi contrattualmente richiesti con le procedure generali del sistema qualità e gestione dei rischi del Fornitore già esistenti;
- esplicitare le disposizioni organizzative, metodologiche e procedurali adottate dal Fornitore, allo scopo di raggiungere gli obiettivi tecnici e di qualità contrattualmente definiti;
- esplicitare per ogni servizio, processo, procedure operative, deliverable documentali del servizio, eventi comunicativi e autorizzativi, matrice RACI e indicatori di qualità;
- esplicitare le disposizioni organizzative e metodologiche adottate dal Fornitore, allo scopo di determinare la più idonea soluzione tecnica ed economica per l'Amministrazione in ciascun servizio affidato e determinare dimensionamenti accurati ed affidabili;
- dettagliare i metodi di lavoro messi in atto dal Fornitore, facendo riferimento a procedure relative al proprio sistema, e perciò descritte nel Manuale Qualità aziendale, o a procedure sviluppate per lo specifico contrattuale, a supporto delle attività in esso descritte (in questo caso da allegare al piano);
- garantire il corretto e razionale evolversi delle attività contrattualmente previste, nonché la trasparenza e la tracciabilità di tutte le azioni messe in atto dalle parti in causa;
- rispettare quanto previsto dalla normativa di riferimento.

Componenti essenziali e organizzazione del Piano della Qualità:

- finalità e obiettivi: descrizione degli scopi del documento, con specifica illustrazione delle ragioni e dei traguardi che ne motivano l'adozione;
- quadro documentale di riferimento: censimento delle fonti contrattuali, tecniche e normative necessarie a supportare e garantire la conformità e la coerenza del piano;

- funzioni, compiti e responsabilità: individuazione degli attori chiave, con specifica definizione delle mansioni assegnate e delle modalità di interazione reciproca;
- fasi operative e cicli di vita: determinazione dell'iter delle attività, dei parametri di conclusione e della documentazione, segnalando eventuali deroghe ai modelli standard;
- parametri e metriche di qualità: definizione degli indicatori di performance, delle relative soglie critiche e degli indici applicati al contesto operativo;
- monitoraggio, riesame e validazione: definizione delle metodologie di controllo, dei test di verifica e dei sistemi di misurazione per l'adempimento dei livelli qualitativi;
- manutenzione ed evoluzione del piano: descrizione degli aggiornamenti a fronte di innovazioni metodologiche o tecnologiche, con indicazione dei soggetti incaricati della gestione e della revisione.

Il Piano della Qualità Generale deve essere presentato all'Amministrazione e da essa approvato entro i primi **30 giorni** solari dalla data di sottoscrizione del Contratto, descrivendo soprattutto i processi operativi e documentali relativi a ciascuno dei servizi oggetto del presente documento, con particolare riferimento alle procedure di interazione tra l'Amministrazione (o terzi designati) e i fornitori.

## 4.3 Piano di Subentro

La fase di subentro si sviluppa dalla data di efficacia del Contratto fino alla data di effettiva presa in carico dell'erogazione dei servizi da parte dei Fornitori e si pone l'obiettivo di permettere il passaggio di consegne tra la struttura di servizio precedente all'efficacia del Contratto e la nuova. La durata di tale fase è fissata in **3 mesi**, salvo diversa indicazione dell'Amministrazione.

Il Piano di Subentro, distinto per servizio, dovrà contenere il dettaglio delle attività che devono essere espletate ad inizio Contratto, la relativa tempificazione e le stime di impegno.

In particolare, dovranno essere esplicitate le risorse professionali ed il loro successivo impiego nei servizi, le attività, i tempi, gli strumenti offerti e quanto necessario alla completa presa in carico di tutti i servizi e predisposizione degli strumenti, delle soluzioni e delle migliorie offerte.

Per le risorse impiegate nei servizi a carattere continuativo e per tutti i referenti dovranno essere forniti i relativi Curricula Vitae secondo quanto riportato nel capitolo 4.6.

Coerentemente con le caratteristiche offerte dai Fornitori e concordate con l'Amministrazione, il Piano dovrà riportare:

- descrizione delle attività di set-up e di subentro;
- nominativo dei Referenti coinvolti nelle attività;
- impegno in GGP, stimato ed effettivo, suddiviso per mese e figura professionale, ove applicabile;
- gantt delle attività, contenente date di inizio e fine, previste ed effettive, delle singole attività/consegne.

Per la parte di stato di avanzamento le informazioni da riportare riguardano:

- data a cui si riferisce lo stato di avanzamento;
- percentuale di avanzamento delle singole attività;
- razionali di ripianificazione, preventivamente concordate con l'Amministrazione, scostamento eventuale delle date, dell'impegno e del volume;
- vincoli/criticità e relative azioni da intraprendere e/o intraprese.

Nel piano si dovranno prevedere almeno le seguenti fasi:

- fase 1: setup del processo
- fase 2: pianificazione di dettaglio
- fase 3: affiancamento e formazione
- fase 4: presa in carico dei tool e strumenti applicativi indicati nel cap. 2.2
- fase 5: conclusione

## 4.4 Piano di Trasferimento Know-How

I Fornitori uscenti, saranno tenuti a pianificare il passaggio di tutte le conoscenze relative ai servizi della presente fornitura mediante la redazione di un Piano di Trasferimento di Know-How. Tale piano dovrà essere presentato entro **180 giorni solari** dalla fine del contratto e dovrà essere approvato dall'Amministrazione.

L'Amministrazione potrà richiedere il Piano anche in caso di cessazione anticipata del rapporto contrattuale.

Il Piano di Trasferimento del Know-How dovrà contenere nel dettaglio:

- una presentazione esaustiva degli aspetti organizzativi, amministrativi e tecnici della fornitura, dei servizi e processi di riferimento;
- la verifica e consegna di tutti i documenti previsti dal presente Contratto;
- la presentazione degli aspetti di criticità di ogni servizio/processo con l'esposizione chiara delle soluzioni proposte ed attuate durante la fornitura;
- la presentazione delle modalità organizzative, degli obiettivi e delle risorse impiegate per la conduzione della fornitura.

Inoltre, coerentemente con le caratteristiche del Know-How da trasferire, il Piano dovrà contenere:

- descrizione delle attività necessarie al passaggio di consegne;
- nominativo dei referenti coinvolti nelle attività;
- impegno in GGP, stimato ed effettivo, suddiviso per mese e figura professionale, ove applicabile;
- gantt delle attività, contenente date di inizio e fine, previste ed effettive, delle singole attività.

Per la parte di stato di avanzamento le informazioni da riportare riguardano:

- data a cui si riferisce lo stato di avanzamento;
- percentuale di avanzamento delle singole attività;
- razionali di ripianificazione, preventivamente concordate con l'Amministrazione, scostamento eventuale delle date, dell'impegno e del volume;
- vincoli/criticità e relative azioni da intraprendere e/o intraprese.

## 4.5 Rendicontazione attività e risorse (Stato Avanzamento Attività)

I Fornitori saranno tenuti a consegnare con frequenza mensile il **Rendiconto attività e risorse**, fornendo tempestivamente indicazioni sulle attività concluse ed in corso, relativamente a tutti i servizi inclusi nella fornitura, esplicitando gli impegni in GG/PP rendicontati nel mese di riferimento, le risorse impegnate e le attività concluse e collaudate nel mese di riferimento, con la relativa dimensione, la percentuale di avanzamento di tutte le attività, descrivendo eventuali criticità/ritardi e le relative azioni di recupero.

Il Fornitore deve consegnare, con cadenza trimestrale ed entro il quinto giorno lavorativo del mese successivo al trimestre di riferimento, il Rapporto Indicatori di Qualità della Fornitura, che contiene la rendicontazione dei Livelli di Servizio conseguiti nei 3 mesi precedenti, ed i servizi che verranno fatturati.

Il documento dovrà essere esplicitamente approvato dall'Amministrazione entro 10 giorni lavorativi dalla consegna.

Il Rendiconto delle Attività e delle Risorse contiene per ogni servizio/attività le sezioni di stato di avanzamento delle attività e di rendiconto delle Risorse impegnate.

La sezione relativa allo stato di avanzamento delle attività dovrà contenere le seguenti informazioni:

- data a cui si riferisce lo stato di avanzamento;
- dettaglio attività svolte.

La sezione relativa al rendiconto delle risorse impegnate dovrà comporsi da una parte analitica ed una sintetica.

La parte analitica contenente:

- elenco del personale impiegato con l'indicazione del profilo professionale ricoperto;
- dettaglio in ore del tempo impiegato da ciascuna risorsa per ogni attività svolta, specificando l'eventuale estensione o reperibilità (ove applicabile).

Nella parte sintetica, che deve popolarsi in maniera automatica a partire dalla parte analitica del Rendiconto Risorse, dovrà essere aggiornato il riepilogo a livello di anno/mese, fornendo in particolare:

- macro-attività a carattere continuativo (il livello di aggregazione delle singole attività viene concordato con il DEC);
- mese/anno di riferimento;
- giorni impiegati per ogni macro-attività, distinti per figura professionale.

Trimestralmente il Rendiconto Attività e Risorse deve contenere anche la misurazione dei Livelli di Servizio illustrati nell'Allegato C1 "Indicatori di Qualità" riferiti al trimestre precedente.

Il documento dovrà illustrare per ciascun indicatore almeno:

- la scheda dell'indicatore;
- il periodo di riferimento della misura;
- il riferimento agli strumenti di misura utilizzati;
- i dati rilevati;
- il valore rilevato dell'indicatore di Qualità;
- l'eventuale scostamento dal valore di soglia;
- l'eventuale razionale di scostamento dai valori di soglia.

## 4.6 Curriculum Vitae delle risorse

Il presente capitolo stabilisce i requisiti per la presentazione del Curriculum Vitae (CV) delle risorse umane che i Fornitori si impegnano a mettere a disposizione per l'esecuzione dei servizi oggetto della gara. La qualità, l'esperienza e le competenze delle risorse assegnate rappresentano un elemento fondamentale per il successo del progetto e per il rispetto dei tempi e degli standard di qualità richiesti dall'Amministrazione.

I Fornitori dovranno presentare un elenco dettagliato delle risorse che saranno impegnate nel progetto, specificando per ciascuna:

- Nome e cognome;
- Ruolo specifico e responsabilità all'interno del progetto;
- Qualifiche professionali (titoli di studio);
- Esperienza professionale rilevante per il progetto (inclusi progetti simili);
- Eventuali competenze aggiuntive (lingue parlate, software utilizzati, ecc.);

A ogni curriculum devono essere allegate le seguenti informazioni:

● descrizione sintetica autocertificata delle attività professionali svolte negli ultimi 24 mesi, contenente l'indicazione del datore di lavoro, l'azienda presso cui si è svolto il servizio, la durata della prestazione e la qualifica professionale ricoperta;

● certificazioni conseguite in ambito IT Service Management, Sicurezza, Compliance e Audit e Project Management quali ad esempio ITIL, PMP, ISO 27001 o ulteriori titoli equivalenti.

Con particolare riferimento alle certificazioni delle risorse, dovranno essere necessariamente indicate:

- data di conseguimento;

- data di scadenza delle stesse.

Inoltre, ogni **6 mesi** l'Amministrazione, si riserva di effettuare delle verifiche sulle certificazioni delle risorse, tramite la richiesta dei profili con le certificazioni. È prevista la possibilità, di effettuare dei colloqui alle risorse dell'organizzazione del Fornitore. Durante la verifica da parte dell'Amministrazione, qualora le certificazioni fossero scadute e non rinnovate, l'Amministrazione si riserverà la facoltà di applicare eventuali penali.

**Censimento delle risorse**

Il Fornitore dovrà curare la predisposizione e l'aggiornamento di un Registro del Personale riportante, almeno, le seguenti informazioni:

- Area di impiego;
- Ruolo;
- Principali responsabilità;
- Data inizio;
- Data fine (eventuale);
- Motivo sostituzione (eventuale);
- Risorsa sostituente (eventuale).

Tale elenco dovrà essere messo a disposizione dell'Amministrazione ed aggiornato alla data della richiesta, tramite un ambiente condiviso.

**Sostituzione delle risorse**

Nel caso di sostituzione di risorse in corso di esecuzione del Contratto dovranno essere presentati, per accettazione da parte dell'Amministrazione i CV delle risorse inserite, in possesso degli stessi o superiori requisiti delle risorse da sostituire, con un preavviso minimo di 15 giorni solari ai fini dell'approvazione da parte dell'Amministrazione.

In caso di sostituzione della risorsa, la fase di Training on the Job e affiancamento alla risorsa uscente per il passaggio di conoscenze di durata non inferiore a 5 giorni lavorativi è a carico del Fornitore stesso; pertanto, i costi relativi alla risorsa entrante non potranno essere addebitati all'Amministrazione.

Nel caso in cui il Fornitore proceda alla sostituzione senza aver ottenuto la necessaria valutazione preventiva e autorizzazione formale da parte dell'Amministrazione, quest'ultima si riserva il diritto di applicare le penali eventualmente previste (vedi Allegato C1 - Indicatori di Qualità).

Parimenti, si dovrà provvedere all'aggiornamento del Registro del Personale.

Modalità di presentazione

I CV delle risorse devono essere inviati in formato elettronico (PDF) e dovranno rispettare i seguenti requisiti:

- ogni CV dovrà essere redatto in lingua italiana o, qualora specificato, in lingua inglese;

- ogni CV dovrà essere stilato secondo lo standard europeo con dichiarazione di autorizzazione al trattamento dei dati personali;
- ogni CV dovrà essere strutturato in modo chiaro, con evidenza dei punti di forza e delle esperienze più rilevanti;
- il Fornitore dovrà attestare che tutte le informazioni contenute nei CV siano veritiere e che le risorse dichiarate siano effettivamente disponibili per il progetto;
- ogni CV del personale che prenderà parte alla fase di subentro dovrà essere consegnato entro i primi 10 giorni solari dalla data di sottoscrizione del Contratto;
- i CV del personale eventualmente non coinvolto nella fase di subentro, ma che sarà operativo nelle attività di esecuzione post avvio, dovranno essere consegnati entro i primi 30 giorni solari dalla data di fine periodo di subentro.

## APPENDICE A – Perimetro della Constituency e Gruppi di Appartenenza

La presente Appendice definisce il perimetro completo degli Enti (Constituency) destinatari dei servizi del CSIRT Regionale.

Al fine di erogare un modello di servizio scalabile e modulare, gli Enti sono stati suddivisi in **5 Gruppi di rischio** dal più al alto al più basso. L'assegnazione di ciascun Ente al proprio gruppo di riferimento è stata effettuata valutando quattro dimensioni principali: la tipologia/dimensione dell'Ente, la presenza di risorse IT interne, il livello di maturità nella gestione della cybersecurity e, con un peso preponderante, il livello di rischio legato ai dati trattati e ai servizi erogati.

Il **Gruppo 1** (rischio più alto) è dedicato specificamente agli Enti dell'area Sanità e Sociale e all'Amministrazione Regionale.

Di seguito si riporta la tabella riepilogativa con tutti gli Enti ordinati per Gruppo di appartenenza:

| GRUPPO DI APPARTENENZA | DENOMINAZIONE ENTE | SOGGETTO NIS | TIPOLOGIA / NOTE |
|---|---|---|---|
| **GRUPPO 1** | Regione del Veneto | Essenziale | Capofila / Coordinamento |
| **GRUPPO 1** | Azienda Zero | Essenziale | Hub Sanitario Regionale |
| **GRUPPO 1** | ULSS 1 – Dolomiti | Essenziale | Ente Sanitario |
| **GRUPPO 1** | ULSS 2 – Marca Trevigiana | Essenziale | Ente Sanitario |
| **GRUPPO 1** | ULSS 3 – Serenissima | Essenziale | Ente Sanitario |
| **GRUPPO 1** | ULSS 4 – Veneto Orientale | Essenziale | Ente Sanitario |
| **GRUPPO 1** | ULSS 5 – Polesana | Essenziale | Ente Sanitario |
| **GRUPPO 1** | ULSS 6 – Euganea | Essenziale | Ente Sanitario |

| | | | |
|---|---|---|---|
| **GRUPPO 1** | ULSS 7 – Pedemontana | Essenziale | Ente Sanitario |
| **GRUPPO 1** | ULSS 8 – Berica | Essenziale | Ente Sanitario |
| **GRUPPO 1** | ULSS 9 – Scaligera | Essenziale | Ente Sanitario |
| **GRUPPO 1** | Azienda Ospedaliera Padova (AOPD) | Essenziale | Ente Sanitario |
| **GRUPPO 1** | Azienda Ospedaliera Verona (AOVR) | Essenziale | Ente Sanitario |
| **GRUPPO 1** | Istituto Oncologico Veneto (IOV) | Essenziale | Ente Sanitario |
| **GRUPPO 2** | Veneto Lavoro | - | Ente Strumentale |
| **GRUPPO 2** | AVEPA | - | Ente Strumentale |
| **GRUPPO 2** | ARPAV | - | Ente Strumentale |
| **GRUPPO 2** | Consorzio Arsenàl.it | - | Ente Strumentale |
| **GRUPPO 3** | Consiglio Regionale del Veneto | Importante | Altro Ente Regionale |
| **GRUPPO 3** | Veneto Strade SpA | Essenziale | Società Partecipata |
| **GRUPPO 3** | Infrastrutture Venete | - | Società Partecipata |
| **GRUPPO 3** | Veneto Innovazione | - | Società Partecipata |
| **GRUPPO 3** | Istituto Zooprofilattico Sperimentale delle Venezie | Importante | Ente sanitario pubblico di controllo, ricerca e servizi negli ambiti della salute animale, dei rischi alimentari e delle zoonosi |
| **GRUPPO 4** | ESU Padova | - | Ente per il Diritto allo Studio |

| | | | |
|---|---|---|---|
| **GRUPPO 4** | ESU Venezia | - | Ente per il Diritto allo Studio |
| **GRUPPO 4** | ESU Verona | - | Ente per il Diritto allo Studio |
| **GRUPPO 4** | Veneto Agricoltura | - | Ente Strumentale |
| **GRUPPO 4** | ATER Belluno | - | Ente Edilizia Residenziale |
| **GRUPPO 4** | ATER Padova | - | Ente Edilizia Residenziale |
| **GRUPPO 4** | ATER Rovigo | - | Ente Edilizia Residenziale |
| **GRUPPO 4** | ATER Treviso | - | Ente Edilizia Residenziale |
| **GRUPPO 4** | ATER Venezia | - | Ente Edilizia Residenziale |
| **GRUPPO 4** | ATER Verona | - | Ente Edilizia Residenziale |
| **GRUPPO 4** | ATER Vicenza | - | Ente Edilizia Residenziale |
| **GRUPPO 5** | Parco Regionale Fiume Sile | - | Ente Parco |
| **GRUPPO 5** | Parco Regionale Colli Euganei | - | Ente Parco |
| **GRUPPO 5** | Parco Regionale Delta del Po | - | Ente Parco |
| **GRUPPO 5** | Istituto Regionale Ville Venete | - | Ente Strumentale |
| **GRUPPO 5** | Veneto Acque | - | Società Partecipata |
| **GRUPPO 5** | Veneto Sviluppo | - | Società Partecipata |
| **GRUPPO 5** | Veneto Edifici Monumentali | - | Società Partecipata |

**Definizione dei gruppi**

Al fine di coadiuvare la definizione del modello organizzativo e operativo del CSIRT, sulla base degli esiti dell'analisi, è stato effettuato un raggruppamento degli enti coinvolti in funzione di alcuni criteri di seguito esplicitati e rapportati al loro relativo peso.

In particolare, al fine di procedere al raggruppamento degli enti sono state prese in considerazione e valutate le seguenti dimensioni:

- Tipo Ente / N. di dipendenti.
- Presenza di risorse interne per la gestione IT /Cybersecurity.
- Livello di maturità di gestione della cybersecurity.
- Livello di rischio (alto, medio o basso) per dati trattati/ tipologia di servizi erogati.

Il **livello di maturità**, utilizzato come parametro per la classificazione degli enti, rappresenta il livello di maturità attuale.

Non si esclude la possibilità di cambiamenti dovuti a progetti in corso, non ancora finalizzati.

I parametri utilizzati per la definizione dei gruppi non risultano esaustivi e comprensivi di tutte le casistiche possibili, per tale motivo, in caso di introduzione di un nuovo ente, quest'ultimo sarà valutato e contestualizzato dando priorità al livello di rischio.

Per tale motivo sono stati definiti dei pesi per ognuna delle metriche sopra rappresentate:

- Livello di Rischio per dati trattati / tipologia di servizi erogati: **34%**
- Numero di Dipendenti: **22%**
- Livello di maturità: **22%**
- Presenza di risorse interne per la gestione dell'IT/ Cybersecurity: **22%**

## Metriche per la definizione dei gruppi di appartenenza degli enti

| 22% | TIPO DI ENTE – N° Dipendenti | |
|---|---|---|
| Grande | ➢ | N° DIP > 300 |
| Medio | ➢ | 15 < N° DIP < 300 |
| Piccolo | ➢ | N° DIP < 15 |

| LIVELLO DI MATURITA' DI GESTIONE DELLA CYBERSECURITY | | 22% |
|---|---|---|
| AVVIATO | ➢ | L'implementazione dei controlli di sicurezza si avvale di processi, procedure e soluzioni tecniche definite |
| DEFINITO | ➢ | L'implementazione dei controlli di sicurezza si avvale di processi, procedure e soluzioni tecniche parzialmente definiti |
| CONSIDE-RATO | ➢ | L'implementazione dei controlli è affidata a processi, procedure e soluzioni tecniche con risultati non prevedibili, non documentati, non organizzati e spesso eseguiti su richiesta |

| 22% | RISORSE INTERNE PER LA GESTIONE IT / CYBER | |
|---|---|---|
| SI | ➢ | Sono presenti delle risorse demandate alla gestione IT |
| No | ➢ | La gestione delle risorse IT è demandata a fornitori esterni |

| LIVELLO DI RISCHIO PER DATI TRATTATI/ TIPOLOGIA DI SERVIZI EROGATI | | 34% |
|---|---|---|
| ALTO | ➢ | Livello di rischio Alto per il tipo di dati trattati/ tipologia di servizi erogati |
| MEDIO | ➢ | Livello di rischio Medio per il tipo di dati trattati/ tipologia di servizi erogati |
| BASSO | ➢ | Livello di rischio Basso per il tipo di dati trattati/ tipologia di servizi erogati |

## Gruppi afferenti al CERT Regionale

| | Tipo di Ente | Risorse Interne IT | Livello di Maturità | Livello di Rischio |
|---|---|---|---|---|
| GRUPPO 1 | Grande | SI | Avviato | Alto |
| GRUPPO 2 | Grande | SI | Avviato | Medio |
| GRUPPO 3 | Medio | SI | Avviato | Medio |
| GRUPPO 4 | Medio | SI | Definito | Medio |
| GRUPPO 5 | Piccolo | NO | Considerato | Basso |

Firma BORGO IDELFO
Data 22-07-2026