



**GARA A PROCEDURA APERTA AI SENSI DEL  
D.LGS. 36/2023 E S.M.I., PER LA CONCLUSIONE DI  
UN ACCORDO QUADRO PER OGNI LOTTO AVENTE  
AD OGGETTO L’AFFIDAMENTO DI SERVIZI  
MANAGED SECURITY SERVICES DA REMOTO, DI  
GOVERNANCE, ANALISI DEL RISCHIO E  
CONTROLLO PER LE PUBBLICHE  
AMMINISTRAZIONI (ID 2737)**

**CAPITOLATO TECNICO SPECIALE  
LOTTI 1 E 2**

**Classificazione Consip: Ambito pubblico**

## Indice

1.	SCOPO DEL DOCUMENTO	5
2.	OGGETTO	5
3.	DESCRIZIONE DEI SERVIZI	6
3.1	Superficie di attacco digitale	7
3.2	Lx.S1 - Security Operation Center (SOC)	8
	Metrica di dimensionamento e modalità di remunerazione	9
3.3	Lx.S2 - Next Generation Firewall (NGFW)	10
	Metrica di dimensionamento e modalità di remunerazione	11
3.4	Lx.S3 - Web Application Firewall and API Protection (WAAP)	12
	Requisiti tecnico-funzionali del servizio	12
	Metrica di dimensionamento e modalità di remunerazione	12
3.5	Lx.S4 – Secure Web Gateway (SWG)	13
	Requisiti tecnico-funzionali del servizio	13
	Metrica di dimensionamento e modalità di remunerazione	14
3.6	Lx.S5 – Secure E-Mail Gateway (SEG)	14
	Requisiti tecnico-funzionali del servizio	14
	Metrica di dimensionamento e modalità di remunerazione	15
3.7	Lx.S6 – Cloud Access Security Broker (CASB)	16
	Requisiti tecnico-funzionali del servizio	16
	Metrica di dimensionamento e modalità di remunerazione	17
3.8	Lx.S7 – Zero Trust Network Access (ZTNA)	18
	Requisiti tecnico-funzionali del servizio	18
	Metrica di dimensionamento e modalità di remunerazione	18
3.9	Lx.S8 - Endpoint Protection (EPP)	19
	Requisiti tecnico-funzionali del servizio	19
	Metrica di dimensionamento e modalità di remunerazione	20
3.10	Lx.S9 - Server Protection Platform (SPP)	20
	Requisiti tecnico-funzionali del servizio	20
	Metrica di dimensionamento e modalità di remunerazione	21
3.11	Lx.S10 - Anti-Advanced Persistent Threat (anti-APT)	22
	Requisiti tecnico-funzionali del servizio	22
	Metrica di dimensionamento e modalità di remunerazione	23
3.12	Lx.S11 - Threat Intelligence & Vulnerability Data Feed	23
	Requisiti tecnico-funzionali del servizio	23
	Metrica di dimensionamento e modalità di remunerazione	24
3.13	Lx.S12 - Supporto specialistico	25

	Requisiti tecnico-funzionali del servizio	25
	Figure professionali	25
	Metrica di dimensionamento e modalità di remunerazione	25
3.14	Modalità di erogazione in configurazione ibrida o on-premise	26
<b>4</b>	<b>REQUISITI DI ESECUZIONE</b>	<b>27</b>
4.1	ISO 9001	27
4.2	ISO 27001	27
4.3	ISO 14001	28
4.4	DNSH	30
4.5	Info-sharing con l'Agenzia Nazionale per la Cyber sicurezza	31
<b>5</b>	<b>CENTRI SERVIZI</b>	<b>33</b>
5.1	Sistema di Gestione della Sicurezza delle Informazioni (ISMS)	35
5.2	Piano di sicurezza dei Centri Servizi	38
<b>6</b>	<b>ADEMPIMENTI A CARICO DEL FORNITORE</b>	<b>41</b>
6.1	SERVICE-DESK	41
6.2	GESTIONE DEGLI INCIDENTI DI SICUREZZA	42
<b>7</b>	<b>FASI OPERATIVE DELLA FORNITURA</b>	<b>48</b>
7.1	Presenza in carico e startup	48
7.2	Modalità di attivazione dei servizi	49
7.3	Fine fornitura	50
7.4	Exit Strategy e Grace Period	51
<b>8</b>	<b>MODALITÀ DI EROGAZIONE</b>	<b>53</b>
8.1	Risorse da impiegare nell'affidamento dei servizi	53
8.2	Competenze richieste	54
8.3	Comunicazioni e Approvazioni	55
8.4	Modalità di Approvazione	55
8.5	Verifiche di conformità	56
8.6	Azioni contrattuali	56
	Rilievi	56
	Penali	57
8.7	Monitoraggio	57
	Reportistica e strumenti di monitoraggio	57
8.8	Dimensionamento dei servizi	58
8.9	Pianificazione e Consuntivazione	60

	Piano della Qualità Generale dell'Accordo quadro	60
	Piano della Qualità Specifico di Contratto esecutivo	61
	Piani di Lavoro	61
	Stato Avanzamento Lavori	62
	Consuntivazione	62
8.10	Orario di erogazione dei servizi	62

## 1. SCOPO DEL DOCUMENTO

Il presente capitolato è parte integrante della documentazione di gara e definisce le caratteristiche e i requisiti per l'affidamento dei servizi Managed Security Services da remoto per le Pubbliche Amministrazioni.

Le prescrizioni contenute nel presente capitolato tecnico, ivi incluse le appendici sotto richiamate, rappresentano requisiti minimi della fornitura.

Ciò comporta che:

- il non rispetto in fase di offerta determinerà l'esclusione dalla procedura di gara;
- il non rispetto in fase di esecuzione costituirà inadempimento contrattuale e comporterà l'applicazione delle sanzioni contrattualmente previste o comunque di un rilievo sulla fornitura in assenza di azioni specifiche.

Sono parti integranti del presente Capitolato Tecnico Speciale le seguenti Appendici:

Appendice 1 – Indicatori di Qualità - Lotti 1 e 2;

Appendice 2 – Profili Professionali - Lotti 1 e 2.

## 2. OGGETTO

Relativamente ai **Lotti 1 e 2**, l'oggetto della fornitura comprende i servizi indicati nella seguente tabella:

ID Servizio	Servizio
Lx.S1	Security Operation Center (SOC)
Lx.S2	Next Generation Firewall (NGFW)
Lx.S3	Web Application Firewall and API protection (WAAP)
Lx.S4	Secure Web Gateway (SWG)
Lx.S5	Secure E-mail Gateway (SEG)
Lx.S6	Cloud Access Security Broker (CASB)
Lx.S7	Zero Trust Network Access (ZTNA)
Lx.S8	End Point Protection (EPP)
Lx.S9	Server Protection Platform (SPP)
Lx.S10	Anti-Advanced Persistent Threat (anti-APT)
Lx.S11	Threat Intelligence & Vulnerability Data Feed
Lx.S12	Supporto specialistico

*Tabella 1 – Elenco servizi*

Il codice identificativo di ciascun Servizio (ID) è una stringa così composta:

- Lx; ove x è l'identificativo del Lotto che può assumere valore 1 o 2;
- Sn; ove n è il numero progressivo del Servizio.

### 3. DESCRIZIONE DEI SERVIZI

La fornitura di servizi di sicurezza da remoto ha l'obiettivo di assicurare, mediante l'utilizzo di risorse, strumenti e figure professionali in logica di servizio, la protezione e la difesa del sistema informativo dell'Amministrazione beneficiaria.

I servizi di sicurezza da remoto dovranno essere erogati dal Fornitore in modalità continuativa secondo un modello "**Managed Security Services**<sup>1</sup>" mediante i Centri Servizi messi a disposizione del Fornitore.

Pertanto, il Fornitore, in coerenza con i requisiti del presente Capitolato, dovrà garantire:

- la disponibilità del servizio, intesa come erogazione continuativa del servizio alle Amministrazioni beneficiarie nonché manutenzione delle componenti infrastrutturali hardware e software necessarie alla corretta funzionalità del servizio;
- la gestione operativa del servizio oggetto di fornitura, intesa come attività di configurazione, amministrazione, manutenzione, aggiornamento e monitoraggio dello stesso.

Il Fornitore dovrà adottare tutte le misure necessarie per garantire scalabilità, performance e resilienza delle infrastrutture che sottendono la continuità di erogazione dei servizi, nonché garantire la riservatezza e protezione dei dati dell'Amministrazione.

A tal fine è di fondamentale importanza che, durante la fase di erogazione dei servizi oggetto di fornitura, il Fornitore sia costantemente interfacciato con le strutture tecniche dell'Amministrazione beneficiaria, in modo da poter contribuire alla realizzazione delle strategie di cyber security adottate, alla protezione e alla difesa del sistema informativo dell'Amministrazione.

I servizi dovranno essere erogati mediante l'impiego di personale del Fornitore esperto, con elevato grado di specializzazione e con una profonda conoscenza del contesto della sicurezza informatica. Le tecnologie proposte dal Concorrente ed esplicitate in sede di offerta tecnica che sottendono l'erogazione dei servizi oggetto di fornitura dovranno garantire una continua protezione dei perimetri dell'Amministrazione in coerenza con le dinamiche di evoluzione e diversificazione degli attacchi informatici.

Il Fornitore dovrà erogare i servizi tenendo conto del contesto normativo, nonché delle specificità funzionali e tecnologiche dell'Amministrazione contraente; in particolare dovrà essere consentita

---

<sup>1</sup> Si riporta a titolo di esempio la definizione di Managed Security Services Provider proposta da Gartner: un fornitore di servizi di sicurezza gestiti (MSSP) fornisce servizi di monitoraggio e gestione externalizzati di dispositivi e sistemi di sicurezza. I servizi più comuni includono firewall gestiti, rilevamento delle intrusioni, reti private virtuali (VPN), scansione delle vulnerabilità e servizi antivirus. Gli MSSP utilizzano centri operativi di sicurezza ad alta disponibilità (sia presso le proprie strutture che presso altri fornitori di data center) per fornire servizi 24 ore su 24, 7 giorni su 7, progettati per ridurre il numero di personale addetto alla sicurezza operativa che un'azienda deve assumere, formare e mantenere per mantenere un livello di sicurezza accettabile.

Fonte: <https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider>

all'Amministrazione l'attuazione delle misure di sicurezza di cui alle linee guida ACN per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90.

Inoltre, data la rilevanza e la complessità delle tematiche oggetto dei servizi, è richiesta disponibilità, dinamicità, accuratezza e riservatezza nell'esecuzione dei servizi.

Si fa presente che il Fornitore dovrà erogare il servizio nel pieno rispetto dei requisiti definiti nel Piano della qualità generale e di quelli espressi nel Piano di qualità dello specifico Contratto esecutivo, anche in termini di adeguata documentazione e degli elaborati prodotti.

In tutti i casi i deliverable di fornitura del servizio dovranno essere direttamente fruibili da parte dell'Amministrazione, mediante apposito trasferimento di know-how verso il proprio personale o verso terzi da esso indicati, nelle modalità previste dal presente capitolato.

Il Fornitore dovrà prevedere e rendere disponibili, senza alcun onere aggiuntivo per l'Amministrazione, tutti gli strumenti necessari per la produzione dei deliverable, per la stesura ed il tracciamento della documentazione e delle informazioni di dettaglio e al fine di garantire l'accessibilità e l'aggiornamento continuo.

In ogni caso, il Fornitore si impegna a rilasciare ogni deliverable nel formato richiesto dall'Amministrazione.

### **3.1 Superficie di attacco digitale**

L'erogazione dei servizi cyber è volta a consentire alle Amministrazioni la protezione dei propri Asset aziendali riducendo la "superficie di attacco digitale" ovvero l'intera area di un'organizzazione o di un sistema, suscettibile ai cyber attacchi della criminalità informatica, provenienti sia dall'interno che dall'esterno della organizzazione stessa. La superficie di attacco rappresenta quindi l'insieme di tutti i possibili punti di ingresso, o vettori di attacco, che possono potenzialmente consentire agli attori malevoli di ottenere l'accesso non autorizzato a sistemi a dati della Pubblica Amministrazione.

Il perimetro tecnologico della PA rappresenta l'insieme delle infrastrutture hardware e software (di base e applicative).

L'infrastruttura tecnologica dell'Amministrazione può essere concentrata in un'unica sede o distribuita su più sedi tra loro interconnesse; può essere, inoltre, connessa al Sistema Pubblico di Connettività (SPC).

All'interno di ciascuna sede della PA, possono essere presenti reti locali con cablaggi strutturati in fibra ottica e/o in rame, eventualmente articolate in più sotto-reti, sulle quali possono essere attestati non solo i server, ma anche le postazioni client del personale dell'Amministrazione e con eventuali "zone demilitarizzate" (DMZ) per l'accesso a/dall'esterno.

La Pubblica Amministrazione potrà disporre sia di infrastrutture tecnologiche “tradizionali” come anche utilizzare infrastrutture implementate secondo il paradigma del Cloud Computing, eventualmente combinando le due modalità secondo i modelli private cloud, public cloud e ibrido.

### 3.2 Lx.S1 - Security Operation Center (SOC)

#### Requisiti tecnico-funzionali del servizio

Il servizio di “Security Operation Center” (SOC) è il centro da cui vengono forniti i servizi H24 alle Amministrazioni mirato a garantire la corretta operatività dei sistemi attraverso la identificazione, gestione, mitigazione e risoluzione di attacchi informatici che possano compromettere la funzionalità dei sistemi dell’Amministrazione. La sua finalità principale è:

- gestire e monitorare i servizi di sicurezza oggetto di fornitura.
- Collezionare ed analizzare la reportistica e i log assegnando la priorità ai processi di risoluzione e/o mitigazione delle minacce.

Il SOC dovrà essere strutturato almeno nei due seguenti livelli:

- **Security Operation Center di livello 1:** analisi e monitoraggio dei sistemi informatici (Triage degli eventi).
- **Security Operation Center di livello 2:** Incident response.

Il servizio “Security Operation Center” dovrà possedere le seguenti caratteristiche/funzionalità:

- avere la capacità di identificazione, gestione, mitigazione, blocco/rilevazione e risposta possibili agli attacchi rilevati sui sistemi e sulle infrastrutture dell’Amministrazione indicati al par. 3.1.
- Effettuare il monitoraggio in tempo reale tramite alert dell’infrastruttura IT e di Sicurezza al fine di individuare tempestivamente tentativi di intrusione, di attacco o di minaccia dei sistemi.
- Consentire la raccolta centralizzata attraverso anche canali cifrati di tipo SSL dei log e degli eventi generati da applicazioni e sistemi in rete (Security information Event Management - SIEM), da sistemi di sicurezza e non gestiti dell’Amministrazione (ad esempio Firewall, Active Directory).
- Prevedere l’interfacciamento con servizi di Threat Intelligence per l’arricchimento delle informazioni utili alla classificazione di un allarme ed alla identificazione delle minacce più recenti e in particolare ricezione di cyber threat intelligence mediante piattaforma MISP e tramite formato STIIX / TAXII.
- Prevedere l’utilizzo di basi dati di conoscenza quali ad esempio i dati di MITRE ATT&CK utilizzando i dati sempre aggiornati relativi a tattiche, tecniche e mitigazioni delle minacce informatiche.

- Attivare i processi di risposta e risoluzione concordati con la PA a seguito di identificazione di un incidente di sicurezza fornendo tutte le informazioni necessarie per consentire il rispetto degli obblighi normativi in termini di segnalazione da parte della PA agli enti preposti.
- Fornire la disponibilità di un Console di gestione per effettuare nuove richieste di servizi, come ad esempio richieste di analisi di incidenti, installazione di patch di sicurezza, o gestione di vulnerabilità.
- Interagire con la piattaforma di trouble ticket di cui al paragrafo 6.1 per la gestione delle richieste e la definizione degli alert e report.
- Avere la capacità di correlare eventi raccolti dal SIEM, provenienti da fonti eterogenee (esempio firewall, sistemi di endpoint, server).
- Prevedere un cruscotto (dashboard) che fornisca agli analisti, in tempo reale, la situazione dei sistemi di sicurezza categorizzando per tipo di dispositivo la presenza di eventi anomali.
- Fornire supporto operativo per la rilevazione di malware al fine di identificare, insieme all'eventuale supporto specialistico, le corrette politiche di difesa e prevenzione.
- Permettere la produzione di report periodici di sintesi, di incident-report di dettaglio ed istruzioni operative a supporto dell'analisi degli incidenti.
- Prevedere l'accREDITAMENTO alla piattaforma HyperSOC dell'Agenzia per la Cybersicurezza Nazionale (di seguito per brevità ACN) al fine di poter fornire informazioni sugli eventi di sicurezza, opportunamente anonimizzati, rilevati nelle PP.AA. così da potenziare le capacità di monitoraggio e analisi nella PA nel suo complesso, e di ricevere in input regole di detection in formati standard (es. Yara, Sigma e Snort).

### **Metrica di dimensionamento e modalità di remunerazione**

La metrica di dimensionamento del servizio di "Security Operation Center" è: **End-point/anno**, ovvero il numero di end point univoci gestiti in un anno.

secondo le classi di seguito indicate:

- Classe 1: fino a 100 Endpoint;
- Classe 2: fino a 500 Endpoint;
- Classe 3: fino a 1.000 Endpoint;
- Classe 4: fino a 2.000 Endpoint;
- Classe 5: fino a 5.000 Endpoint;
- Classe 6: > 5.000 Endpoint.

Ogni dispositivo che può essere utilizzato per accedere alla rete e ai suoi dati è considerato un endpoint (ad esempio: dispositivi mobili, computer desktop, workstation, macchine virtuali, dispositivi incorporati, server, stampanti, telecamere, dispositivi Internet of Things).

La modalità di remunerazione del servizio di “Security Operation Center” è: **Canone annuale per end-point**.

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

### 3.3 Lx.S2 - Next Generation Firewall (NGFW)

#### Requisiti tecnico-funzionali del servizio

Il servizio di “Next Generation Firewall” (NGFW) dovrà consentire di filtrare tutto il traffico che i dispositivi di rete scambiano sia internamente che esternamente rispetto al perimetro della PA, limitando o bloccando eventi quali accessi non autorizzati, malware o servizi non consentiti, attraverso una serie definita di regole (policy) di controllo degli accessi e tramite l'orchestrazione di più layer di sicurezza, ognuno dedicato a una specifica funzione di controllo.

Il servizio di “Next Generation firewall” dovrà possedere almeno le seguenti caratteristiche/funzionalità:

- Prevedere funzionalità di network firewall (stateful inspection, policy enforcement, packet filtering, DNAT e SNAT, VPN IPSEC client to site e site to site, VPN TLS).
- Prevedere funzionalità di Meccanismi di Intrusion Prevention System (IPS) avanzato, dotati di funzionalità di rilevamento, blocco e tracciamento delle minacce informatiche, attraverso l'adozione di meccanismi di ispezione dei malware basati su firme, rilevamento di anomalie (inclusa l'individuazione di anomalie nei protocolli di rete IP), analisi euristica e comportamentale, con la possibilità di definire firme personalizzate per contrastare attacchi non ancora censiti.
- Implementare WEB/URL Filtering statico e dinamico, con possibilità di controllare le statistiche sulla navigazione, di bloccare l'accesso a particolari siti e creare anche categorie personalizzate.
- Prevedere funzionalità anti-malware sia su base firma che su base comportamentale.
- Prevedere funzionalità anti-spam.
- Prevedere funzionalità di anti-botnet.
- Prevedere funzionalità di sandboxing integrata o su infrastruttura remota del Produttore, ubicata in UE.
- Disporre della tecnologia Deep Packet Inspection per scansionare l'intero payload dei pacchetti.
- Disporre della capacità di ispezione TLS/SSL per l'ispezione del traffico cifrato.
- Disporre della capacità di ispezione del traffico SSH.
- Capacità di controllare le applicazioni con blocco dell'esecuzione in funzione della configurazione impostata dall'Amministratore di Sistema.

- Gestire la QoS band-width con la possibilità di impostare una larghezza di banda minima garantita e un limite massimo di larghezza di banda per il traffico insieme ad un valore di priorità.
- Prevedere la trasmissione di eventi e log alla funzionalità di SIEM del servizio SOC oggetto di fornitura o ad altro strumento di raccolta log, ove disponibile, dell'Amministrazione.
- Prevedere la produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.
- Disporre di funzionalità di accesso selettivo alle applicazioni con modello Zero Trust basata su identificazione dei dispositivi client e autenticazione degli utenti.
- Capacità di analisi del traffico su base geolocalizzazione degli IP e possibilità di filtraggio/blocco.
- Prevedere il supporto di protocolli standard STIX/TAXII e formato dati MISP.
- Prevedere la possibilità di definire da parte della PA un profilo di compliance oggetto di monitoraggio.

#### **Metrica di dimensionamento e modalità di remunerazione**

La metrica di dimensionamento del servizio di "Next Generation Firewall" è: **Throughput**

secondo le seguenti classi:

- Classe 1: fino a 600 Mbps;
- Classe 2: fino a 2 Gbps;
- Classe 3: fino a 4 Gbps;
- Classe 4: fino a 6 Gbps;
- Classe 5: fino a 10 Gbps;
- Classe 6: fino a 20 Gbps;
- Classe 7: fino a 30 Gbps;
- Classe 8: fino a 50 Gbps.

Si precisa che per *Throughput NGFW* si intende il throughput ottenuto con le funzionalità **contemporaneamente attive**, tra le quali rientrano a titolo esemplificativo e non esaustivo l'ispezione *stateful (stateful inspection)*, la prevenzione delle intrusioni (*intrusion prevention – IPS*).

La modalità di remunerazione del servizio di "Next Generation Firewall" è: **Canone annuale per appliance**.

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

### 3.4 Lx.S3 - Web Application Firewall and API Protection (WAAP)

#### Requisiti tecnico-funzionali del servizio

Il servizio di “Web Application Firewall and API Protection” (WAAP) dovrà consentire di filtrare, monitorare e bloccare il traffico HTTP da e verso un servizio applicativo Web e API, esaminando il traffico, utilizzando regole, analisi e firme per rilevare attacchi e quindi proteggendo le stesse Amministrazioni dagli attacchi incorporati nei dati trasmessi dalle applicazioni web.

Il servizio di “Web Application Firewall and API Protection” dovrà possedere le seguenti funzionalità/caratteristiche:

- Prevedere la capacità di protezione dagli attacchi applicativi almeno OWASP TOP 10 (ultima versione disponibile alla data di presentazione offerta).
- Disporre della capacità di ispezione del traffico HTTP/HTTPS.
- Disporre delle funzionalità di protezione delle API web che utilizzano formati strutturati quali JSON e XML, mediante l'analisi dei dati veicolati da questi formati.
- Disporre della capacità di controllo dell'IP Reputation.
- Disporre della capacità di mitigazione degli attacchi bot.
- Disporre della possibilità di definire Blacklist e Whitelist di accesso, anche basandosi sulla georeferenziazione degli IP address
- Prevedere l'implementazione di funzionalità di offloading SSL.
- Consentire il rilevamento e mitigazione di attacchi DDOS di tipo applicativo.
- Disporre di funzionalità di Virtual Patching.
- Disporre di funzionalità di sandboxing.
- Disporre di funzionalità di bilanciamento di livello 7 (modello ISO/OSI) delle applicazioni
- Prevedere la possibilità di importare/esportare feed IoC proprietarie o di terze parti qualificate, quali MISP ACN e CERT- AgID, tramite protocolli standard (STIX/TAXII).
- Prevedere la trasmissione di eventi e log alla funzionalità di SIEM del servizio SOC oggetto di fornitura o ad altro strumento di raccolta log, ove disponibile, dell'Amministrazione.
- Prevedere la produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report) al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.

#### Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento del servizio di “Web Application Firewall and API Protection” è:

##### Throughput

secondo le seguenti classi:

- Classe 1: fino a 500 Mbps;
- Classe 2: fino a 2,5 Gbps;
- Classe 3: fino a 5 Gbps;

- Classe 4: fino a 10 Gbps.

La modalità di remunerazione del servizio di “Web Application Firewall and API Protection” è: **Canone annuale per appliance.**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

### 3.5 Lx.S4 – Secure Web Gateway (SWG)

#### Requisiti tecnico-funzionali del servizio

Il servizio di “Secure Web Gateway” (SWG) consente alle Amministrazioni di proteggersi contro le minacce alla sicurezza online applicando le policy aziendali e filtrando il traffico internet dannoso in tempo reale. Viene bloccato l'accesso ai siti potenzialmente malevoli, applicato il controllo alle applicazioni web e rilevato e filtrato il codice dannoso.

Il servizio “Secure Web Gateway” dovrà possedere le seguenti caratteristiche/funzionalità:

- prevedere il filtraggio:
  - proxy del traffico in modalità trasparente ed esplicita;
  - delle URL;
  - dei contenuti;
  - dei protocolli, tra cui HTTP/HTTPS/FTP;
  - delle applicazioni.
- Consentire la definizione criteri di sicurezza/filtraggio per utente e/o gruppi e definizione di blacklist/whitelist.
- Supportare il PAC file per l'implementazione in modalità esplicita.

Per i PAC file deve essere prevista l'adozione di:

- meccanismi di limitazione degli accessi in scrittura;
- trasmissione protetta su HTTPS.
- Disporre della capacità di Web/URL Filtering basato su categorie predefinite (almeno 80), aggiornate su base necessità e periodicamente almeno ogni 3 mesi.
- Disporre della capacità di identificazione dei comportamenti potenzialmente pericolosi, blocco dei siti potenzialmente malevoli o categorizzati come tali e blocco dei file in base all'estensione.
- Disporre della presenza di un database di identificativi degli attacchi e delle categorie dei siti, aggiornabile anche in base a richieste specifiche dell'Amministrazione.
- Prevedere la funzionalità di protezione Anti Malware, WEB/IP reputation e anti-botnet sul traffico gestito.
- Consentire l'identificazione attacchi di tipo zero-day.
- Disporre della capacità di applicazione delle policy definite anche ai dispositivi offnet. Per tale funzionalità potrà essere previsto l'utilizzo di agent da installare sui dispositivi remoti e che supporti i principali Sistemi Operativi (Windows, MacOS, iOS, Android).

- Disporre della capacità di ispezione TLS/SSL per l'ispezione del traffico cifrato.
- Prevedere la trasmissione di eventi e log alla funzionalità di SIEM del servizio SOC oggetto di fornitura o ad altro strumento di raccolta log, ove disponibile, dell'Amministrazione.
- Prevedere il supporto dei principali meccanismi di autenticazione quali: Kerberos, NTLM, LDAP, AD, SAML.
- Prevedere la produzione di report di sintesi (executive summary) e di dettaglio (technical report).
- Disporre di funzionalità di reportistica attraverso dashboard e API che consenta:
  - il monitor in real-time;
  - la realizzazione di report tramite template predefiniti o personalizzabili;
  - la possibilità di esportare i report.
- Prevedere la possibilità di importare/esportare feed IoC proprietarie o di terze parti qualificate, quali MISP ACN e CERT- AgID, tramite protocolli standard (STIX/TAXII).

#### **Metrica di dimensionamento e modalità di remunerazione**

La metrica di dimensionamento del servizio di "Secure Web Gateway" è: **Numero utenti/anno** secondo le seguenti classi:

- Classe 1 - Fino a 1000 utenti;
- Classe 2 - Fino a 5.000 utenti;
- Classe 3 - Fino a 10.000 utenti;
- Classe 4 - Fino a 20.000 utenti;
- Classe 5 - > 20.000 utenti.

La modalità di remunerazione del servizio di "Secure Web Gateway" è: **Canone annuale per utente**. L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

### **3.6 Lx.S5 – Secure E-Mail Gateway (SEG)**

#### **Requisiti tecnico-funzionali del servizio**

Il servizio di "Secure E-Mail Gateway" (SEG) consente alle Amministrazioni di proteggersi contro le minacce filtrando il traffico della posta elettronica sia in entrata che in uscita impedendo alle minacce di raggiungere il destinatario previsto.

Il servizio "Secure E-Mail Gateway" dovrà possedere le seguenti funzionalità/caratteristiche:

- permettere l'ispezione sulla posta in uscita e in ingresso.
- Permettere il filtraggio dei messaggi indesiderati/sospetti che potrebbero contenere virus, malware o essere parte di attacchi di phishing.

- Prevedere funzionalità di antivirus, anti-phishing, anti-BEC, anti-spoofing, anti-spam e anti-malware in grado di identificare virus, worms, ransomware attraverso il riconoscimento di signature e analisi euristica dei contenuti.
- Consentire il filtraggio da e-mail massive e di marketing.
- Consentire il blocco di e-mail in base alla lingua utilizzata o specifici charset.
- Supportare i protocolli SPF, DKIM o in alternativa del protocollo DMARC e alla compliance delle configurazioni degli stessi protocolli.
- Implementare la crittografia dei messaggi in uscita con protocollo SSL/TLS.
- Implementare la protezione realtime Office 365 attraverso API o SMTP relay.
- Consentire il supporto dei filtri basati sulla reputazione dell'indirizzo IP di provenienza e/o URL.
- Mantenere aggiornamenti delle signature e IOC per identificare e bloccare le e-mail dannose prima che raggiungano le caselle di posta degli utenti.
- Possibilità di bloccare mail contenenti documenti di Office che utilizzino MACRO, segnalando all'amministratore/utente l'avvenuto blocco.
- Permettere l'analisi del contenuto di ogni mail al fine di bloccare virus and malware, garantendo il costante aggiornamento dei "Threat pattern".
- Avere la capacità di trasmissione dei log per l'alimentazione del sistema SIEM.
- Consentire il supporto del protocollo IPv6.
- Disporre di funzionalità di reportistica che consentano:
  - il monitor in real-time attraverso dashboard;
  - la realizzazione di report attraverso template predefiniti;
  - la possibilità di esportare i report.

#### **Metrica di dimensionamento e modalità di remunerazione**

La metrica di dimensionamento del servizio di "Secure E-Mail Gateway" (SEG) è: **Numero utenti/anno**, secondo le seguenti classi:

- Classe 1 - Fino a 1000 utenti;
- Classe 2 - Fino a 5.000 utenti;
- Classe 3 - Fino a 10.000 utenti;
- Classe 4 - Fino a 20.000 utenti;
- Classe 5 - > 20.000 utenti.

La modalità di remunerazione del servizio di "Secure E-Mail Gateway" (SEG) è: **Canone annuale per utente**.

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

### 3.7 Lx.S6 – Cloud Access Security Broker (CASB)

#### Requisiti tecnico-funzionali del servizio

Il servizio di “Cloud Access Security Broker” (CASB) agisce come intermediario tra gli utenti dell’Amministrazione e i servizi cloud, monitorando, controllando e proteggendo l’accesso agli servizi cloud, applicando politiche di sicurezza e prevenendo potenziali rischi per la sicurezza, come fughe di dati o accesso non autorizzato.

Il servizio “Cloud Access Security Broker” dovrà possedere le seguenti funzionalità/caratteristiche:

- garantire almeno un metodo di autenticazione forte basato su SAML o altro metodo di riconoscimento (MFA).
- Monitorare la postura di sicurezza dei dispositivi connessi permettendo il blocco degli accessi in situazioni di potenziale compromissione.
- Disporre di funzionalità di Data Loss Prevention (DLP).
- Disporre della capacità di monitoraggio degli utenti connessi alle applicazioni SaaS indipendentemente dai dispositivi utilizzati.
- Disporre della capacità di monitoraggio continuo e analisi del comportamento utente anche in base a dati storici ad esso relativo, che prenda in considerazione almeno la geolocalizzazione, l’IP e le fasce orarie.
- Garantire la gestione delle policy di accesso alle applicazioni cloud dell’Amministrazione, sia predefinite che personalizzabili, tale da consentire la definizione di criteri basati su parametri quali geolocalizzazione, indirizzi IP, fasce orarie e permessi di accesso alle risorse ed ulteriori parametri definiti dalle esigenze dell’Amministrazione, garantendo al contempo la trasparenza per l’utente finale.
- Disporre della possibilità di installazione di agent su dispositivo e possibilità di accesso clientless (agentless) via browser per supportare architetture BYOD.
- Disporre della funzionalità di reportistica che consentano:
  - il monitor in real-time attraverso dashboard
  - la realizzazione di report attraverso template predefiniti o personalizzabili sia di livello executive che operativa/di dettaglio
  - la possibilità di esportare i report.
- Disporre della capacità di analisi del contenuto e delle attività svolte sulle applicazioni SaaS, incluse Microsoft 365 OneDrive, Sharepoint, Teams, permettendo la rilevazione di minacce.
- Disporre della capacità di rilevazione di tutte le applicazioni cloud dell’Amministrazione, permettendo l’identificazione di Shadow IT.
- Prevedere la trasmissione di eventi e log alla funzionalità di SIEM del servizio SOC oggetto di fornitura o ad altro strumento di raccolta log, ove disponibile, dell’Amministrazione.
- Disporre della capacità di implementare meccanismi di allarmistica configurabili dalla Pubblica Amministrazione, atti a rilevare e segnalare eventi potenzialmente pericolosi quali

comportamenti anomali, compromissioni di dispositivi e applicazioni non autorizzate, con la possibilità di estendere i parametri di rilevamento tramite configurazioni future.

- Disporre della capacità di implementare meccanismi di protezione avanzati contro un'ampia gamma di minacce informatiche, quali malware, phishing, attacchi zero-day e altre minacce emergenti, con la possibilità di aggiornare e integrare costantemente le misure di difesa.
- Disporre della capacità di accesso alle risorse dell'Amministrazione sulla base della profilatura utente.

### **Metrica di dimensionamento e modalità di remunerazione**

La metrica di dimensionamento del servizio di "Cloud Security Access Broker" (CASB) è: **Numero utenti/anno**

secondo le seguenti classi:

- Classe 1 - Fino a 100 utenti;
- Classe 2 - Fino a 500 utenti;
- Classe 3 - Fino a 2.000 utenti;
- Classe 4 - Fino a 5.000 utenti;
- Classe 5 - > 5.000 utenti.

La modalità di remunerazione del servizio di "Cloud Security Access Broker" (CASB) è: **Canone annuale per utente.**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

### 3.8 Lx.S7 – Zero Trust Network Access (ZTNA)

#### Requisiti tecnico-funzionali del servizio

Il servizio di “Zero Trust Network Access” (ZTNA) consente agli utenti della PA di accedere in modo sicuro alle applicazioni interne e servizi da remoto in base a policy di controllo degli accessi.

Il servizio “Zero Trust Network Access” dovrà possedere le seguenti funzionalità/caratteristiche:

- garantire in modo trasparente l'accesso alle sole risorse dell'Amministrazione a cui l'utente è stato autorizzato, su base profilatura.
- Disporre di un meccanismo di autenticazione forte conforme agli standard di sicurezza più elevati, con supporto per metodi quali MFA e SAML, e la possibilità di integrare ulteriori protocolli di autenticazione in base alle evoluzioni normative e tecnologiche.
- Supportare almeno i protocolli: FTP, SSH, RDP, SSL, HTTP/HTTPS.
- Disporre della capacità di disporre di un meccanismo di valutazione continua della postura degli endpoint, che consenta la definizione di criteri di valutazione personalizzabili dall'Amministrazione, quali almeno tipo e versione del sistema operativo, tipo e versione del browser, stato di aggiornamento dell'antivirus e geolocalizzazione, con la possibilità di integrare ulteriori parametri di valutazione in base alle esigenze dell'Amministrazione.
- Disporre della capacità sia di installazione di agent su dispositivo, sia della possibilità di accesso clientless (agentless) via browser.
- Disporre della capacità di supportare i principali Sistemi Operativi (Windows, Linux, macOS).
- Disporre di funzionalità di reportistica che consentano:
  - il monitor in real-time attraverso dashboard;
  - la realizzazione di report attraverso template predefiniti o personalizzabili;
  - la possibilità di esportare i report.
- Garantire la gestione delle policy di accesso alle risorse dell'Amministrazione (infrastrutture, dati e applicazioni), personalizzabili in base alle esigenze dell'Amministrazione, in contesti on-prem, cloud e ibridi.
- Prevedere la trasmissione di eventi e log alla funzionalità di SIEM del servizio SOC oggetto di fornitura o ad altro strumento di raccolta log, ove disponibile, dell'Amministrazione.
- Disporre della capacità di implementare meccanismi di protezione avanzati contro un'ampia gamma di minacce informatiche, quali almeno malware, phishing, attacchi zero-day e altre minacce emergenti, con la possibilità di aggiornare e integrare costantemente le misure di difesa.

#### Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento del servizio di “Zero Trust Network Access” è: **Numero utenti/anno** secondo le seguenti classi:

- Classe 1 - Fino a 100 utenti;

- Classe 2 - Fino a 500 utenti;
- Classe 3 - Fino a 1.000 utenti;
- Classe 4 - Fino a 2.000 utenti;
- Classe 5 - Fino a 5.000 utenti;
- Classe 6 - > 5.000 utenti.

La modalità di remunerazione del servizio di “Zero Trust Network Access” è: **Canone annuale per utente.**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

### 3.9 Lx.S8 - Endpoint Protection (EPP)

#### Requisiti tecnico-funzionali del servizio

Il servizio di “Endpoint protection” (EPP) consente alle Amministrazioni di proteggere i dispositivi collegati alla rete aziendale (ad es. pc desktop, laptop, smartphone, tablet) dall'accesso non autorizzato o dall'esecuzione di software dannoso. La protezione degli endpoint garantisce, inoltre, che i dispositivi raggiungano un livello di sicurezza definito e siano rispondenti ai requisiti di conformità dell'Amministrazione.

Il servizio di “Endpoint protection” dovrà possedere le seguenti funzionalità/caratteristiche:

- supportare gli endpoint con i Sistemi Operativi più diffusi (Windows 11, 10, 8.1, 7, e le versioni più recenti di macOS, Linux, iOS e Android).
- Consentire la protezione dei dispositivi mediante sistemi antimalware (antivirus, antispam), impedendo lo sfruttamento delle carenze di sicurezza e l'accesso non autorizzato.
- Permettere l'ispezione del traffico https. Blocco dell'accesso a siti potenzialmente malevoli e controllo delle applicazioni mobile per evitare attivazioni fraudolente di Active x, Java Script ed eseguibili, rilevando e filtrando il traffico internet dannoso in tempo reale.
- Consentire la conformità alle politiche dell'Amministrazione e quindi la possibilità di verificare se siano applicate le regole previste dalle policy di sicurezza nel dispositivo connesso alla rete dell'Amministrazione, come ad es. utilizzo di un sistema operativo approvato, installazione di una VPN, l'esecuzione di un software antivirus aggiornato e compliance anche per accesso remoto.
- Consentire il monitoraggio Real time delle minacce e protezione da malware basati su file e senza file, identificando gli attacchi in fase iniziale e la risposta rapida ad un'ampia gamma di minacce (Endpoint Detection and Response – EDR).
- Permettere la protezione Anti-Tampering; inibizione dell'interruzione del servizio del sistema di protezione da parte dell'utente.
- Possedere la funzionalità Antimalware signature based aggiornate in modo automatico.

- Possedere la protezione dai ransomware.
- Garantire la visibilità e il controllo delle periferiche collegate agli endpoint, assicurando meccanismi di monitoraggio, applicazione di policy di sicurezza, rilevazione di utilizzi anomali e registrazione degli eventi ai fini di audit e investigazione.
- Permettere di effettuare la Root Cause Analysis.
- Permettere di effettuare delle scansioni in modalità real time, manuale o programmata.
- Permettere di effettuare detection di malware attraverso sorgenti IoC (indicatori di compromissione).
- Disporre della capacità di importare/esportare liste dinamiche di IOC proprietarie o di terze parti certificate tramite protocolli standard (STIX/TAXII).
- Permettere la registrazione di dati di telemetria degli endpoint (almeno connessioni di rete, esecuzione di file, modifiche di file, modifiche di registro).
- Consentire la produzione di reportistica e logging che consentano la realizzazione di report attraverso template predefiniti.

#### **Metrica di dimensionamento e modalità di remunerazione**

La metrica di dimensionamento del servizio di “Protezione endpoint” è: **End-point/anno** secondo le seguenti classi:

- Classe 1 - Fino a 500 End-point;
- Classe 2 - Fino a 1.000 End-point;
- Classe 3 - Fino a 5.000 End-point;
- Classe 4 - > 5.000 End-point.

La modalità di remunerazione del servizio di “Protezione endpoint” è: **Canone annuale per end-point**.

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

### **3.10 Lx.S9 - Server Protection Platform (SPP)**

#### **Requisiti tecnico-funzionali del servizio**

Il servizio di “Server Protection Platform” (SPP) consente alle Amministrazioni di proteggere i server collegati alla rete aziendale dall'accesso non autorizzato o dall'esecuzione di software dannoso. La protezione dei server garantisce, inoltre, il raggiungimento di un livello di sicurezza definito e siano conformi ai requisiti di conformità dell'Amministrazione.

Il servizio di “Server Protection Platform” dovrà possedere le seguenti funzionalità/caratteristiche:

- prevedere il supporto dei server con Sistema Operativo Windows Server (Windows Server 2016 e 2019) e distribuzioni Linux, tra cui Red Hat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server, Amazon Linux, e Oracle Linux.

- Prevedere la protezione dei server mediante sistemi antimalware (esempio antivirus) impedendo lo sfruttamento delle carenze di sicurezza e l'accesso non autorizzato.
- Permettere l'ispezione del traffico https. Blocco dell'accesso a siti potenzialmente malevoli e controllo delle applicazioni mobile per evitare attivazioni fraudolente di Active x, Java Script ed eseguibili, rilevando e filtrando il traffico internet dannoso in tempo reale.
- Consentire la conformità alle politiche dell'Amministrazione e quindi la possibilità di verificare se siano applicate le regole previste dalle policy di sicurezza nel server connesso alla rete dell'Amministrazione, come ad es. utilizzo di un sistema operativo approvato, installazione di una VPN o l'esecuzione di un software antivirus aggiornato.
- Consentire il monitoraggio Real time delle minacce e protezione da malware basati su file e senza file, identificando gli attacchi in fase iniziale e la risposta rapida ad un'ampia gamma di minacce (Endpoint Detection and Response – EDR).
- Possedere funzionalità Antimalware signature based aggiornate in modo automatico.
- Permettere la protezione dai ransomware.
- Permettere il controllo dell'uso dei dispositivi USB e periferiche di archiviazione (ad es. pendrive, hard-disk esterni) prevenendo l'utilizzo non autorizzato monitorando le porte di comunicazione (ad es. USB, SATA).
- Effettuare delle scansioni in modalità real time, manuale o programmata.
- Effettuare la Root Cause Analysis.
- Effettuare detection di malware attraverso sorgenti IoC (indicatori di compromissione).
- Disporre della capacità di importare/esportare liste dinamiche di IOC proprietarie o di terze parti certificate tramite protocolli standard (STIX/TAXII).
- Permettere la registrazione di dati di telemetria degli endpoint (almeno connessioni di rete, esecuzione di file, modifiche di file, modifiche di registro).
- Possedere la funzionalità di reportistica e logging che consentano la realizzazione di report attraverso template predefiniti.

### **Metrica di dimensionamento e modalità di remunerazione**

La metrica di dimensionamento del servizio di "Server Protection Platform" è: **Server/anno** secondo le seguenti classi:

- Classe 1 - Fino a 50 Server;
- Classe 2 - Fino a 100 Server;
- Classe 3 - Fino a 500 Server;
- Classe 4 - > 500 Server.

La modalità di remunerazione del servizio di "Server Protection Platform" è: **Canone annuale per server.**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

### 3.11 Lx.S10 - Anti-Advanced Persistent Threat (anti-APT)

#### Requisiti tecnico-funzionali del servizio

Il servizio di “Anti-Advanced Persistent Threat (anti-APT)” è volto a contrastare le minacce persistenti avanzate (APT) ovvero attacchi informatici non rilevati progettati per rubare dati sensibili, condurre attività di spionaggio informatico o sabotare i sistemi critici per un lungo periodo di tempo.

Il servizio anti-APT identifica file sospetti in base al traffico di rete e ai metadati. All'interno dell'ambiente protetto (sandbox) sarà possibile, esaminare i file e i loro comportamenti per determinare se questi siano o meno malevoli, assegnando loro un grado di severità.

Il servizio di “Anti-Advanced Persistent Threat” (anti-APT) dovrà possedere le seguenti funzionalità/caratteristiche:

- supportare i Sistemi Operativi più diffusi (Windows 11, 10, 8.1, 7, e le versioni più recenti di macOS, Linux, iOS e Android) e del software Microsoft Office.
- Consentire la rilevazione, mediante analisi comportamentale in ambiente sandbox di malware, minacce zero-day e APT.
- Consentire di verificare file attraverso la corrispondenza delle firme di malware in precedenza già analizzati.
- Supportare almeno le seguenti tipologie di file archivi: .zip, .gz, .bz2, eseguibili, .pdf, .jar, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .iso, .img.
- Supportare almeno le seguenti tipologie di file eseguibili: BAT, CMD, DLL, EXE, JAR, JSE, MSI, PS1, UPX, WSF, VBS.
- Supportare i seguenti protocolli e applicazioni: HTTP, FTP, SMTP, IMAP, POP3, SMB.
- Includere la capacità di sottomissione manuale (ad esempio del file sul sistema anti-APT) e automatica (ad esempio mediante integrazione con altri sistemi di analisi) di file e URL, per analizzare e identificare potenziali minacce.
- Permettere l'identificazione, mediante analisi del traffico di rete in ambiente sandbox, di minacce quali: comunicazione C&C, botnet e worm.
- Disporre di funzionalità in ambiente sandbox che consentano di rilevare tecniche di elusione utilizzate dai malware quali: cifratura, compressione e offuscamento del codice.
- Permettere di creare regole di rilevazione personalizzate attraverso YARA e SIGMA Rules.
- Integrare feed di threat intelligence per ricevere informazioni aggiornate sui nuovi malware e altri attacchi informatici mediante formati standard (MISP, STIX, TAXII); il feed fornisce dati in tempo reale sulle minacce, permettendo al sistema di aggiornare la sua conoscenza e di essere più efficace nella rilevazione e gestione degli attacchi APT.
- Creare macchine virtuali personalizzate per l'analisi dei malware nello specifico contesto dell'Amministrazione.
- Avere funzionalità di reportistica che consentano:
  - il monitoraggio in real-time attraverso dashboard;

- realizzare report attraverso template predefiniti;
  - esportare i report.
- Supportare il protocollo IPv6.

### **Metrica di dimensionamento e modalità di remunerazione**

La metrica di dimensionamento del servizio di “Anti-Advanced Persistent Threat” è: **File/ora** secondo le seguenti classi:

- Classe 1: fino a 450 File/ora;
- Classe 2: fino a 1.000 File/ora;
- Classe 3: fino a 2.800 File/ora;
- Classe 4: fino a 4.200 File/ora;
- Classe 5: fino a 5.000 File/ora;
- Classe 6: fino a 8.000 File/ora.

La modalità di remunerazione del servizio di “Anti-Advanced Persistent Threat” è: **Canone annuale per appliance** (espressa in capacità di gestione File/ora).

## **3.12 Lx.S11 - Threat Intelligence & Vulnerability Data Feed**

### **Requisiti tecnico-funzionali del servizio**

Il servizio di “Threat intelligence e Vulnerability data feed” dovrà consentire alle Amministrazioni di ricevere un flusso continuo di dati relativi a minacce e vulnerabilità di sicurezza del Sistema informativo. Devono essere disponibili le informazioni più recenti, permettendo così di prevedere/prevenire le minacce prima che entrino in azione, migliorando gli attuali controlli e le funzionalità forensi.

Il servizio di “Threat intelligence e Vulnerability data feed” dovrà possedere le seguenti funzionalità/caratteristiche:

- rendere disponibili feed di indicatori (ad es., SANS, OSVDB), bollettini, raccolte di informazioni interne ed altre fonti informative (aperte e non).
- Rendere disponibili interfacce di integrazione (API) per l'automazione dei report, consentendo la raccolta di informazioni, come ad es. il numero di volte che una specifica minaccia è stata individuata nel mondo, gli URL contenenti codici dannosi e il comportamento tipico di un malware sul sistema dove è stato individuato.
- Rendere disponibili flussi di Indicatori di Compromissione (domini sospetti, elenchi di hash malware noti, Indirizzi IP associati ad attività dannose, codice condiviso su Pastebin).
- Rendere disponibili vulnerability feed estratti dal National Vulnerability Database (NVD), quali ad es., vulnerabilità JSON, RSS.

### **Metrica di dimensionamento e modalità di remunerazione**

La metrica di dimensionamento del servizio di “Threat Intelligence e Vulnerability Data Feed” è: **Data-Feed/anno**

secondo le seguenti fasce:

- Fascia 1: fino a 10 Data feed;
- Fascia 2: fino a 50 Data feed;
- Fascia 3: > 50 Data feed.

La modalità di remunerazione del servizio di “Threat Intelligence e Vulnerability Data Feed” è: **Canone annuale per Data-Feed.**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

### 3.13 Lx.S12 - Supporto specialistico

#### Requisiti tecnico-funzionali del servizio

Il servizio "Supporto specialistico" dovrà fornire all'Amministrazione un supporto tecnico funzionale all'attivazione dei servizi da remoto oggetto di fornitura.

Il servizio è erogato a richiesta mediante la messa a disposizione di figure professionali da parte del Fornitore. Il dimensionamento complessivo del servizio è effettuato dall'Amministrazione, che determina il numero di giorni/persona, per i diversi profili professionali, ritenuti necessari nel corso dell'intera durata contrattuale.

Si riporta a titolo esemplificativo e non esaustivo alcune attività che possono essere svolte attraverso il servizio:

- studio di fattibilità relativamente all'introduzione/evoluzione dei servizi oggetto di acquisizione e ricadenti nell'ecosistema dell'Amministrazione;
- analisi e supporto alla migrazione dei servizi di sicurezza dell'Amministrazione verso i servizi oggetto di fornitura, per le fasi di analisi e supporto alla configurazione;
- supporto alle attività di delivery dei servizi oggetto di fornitura durante le operazioni di migrazione.

#### Figure professionali

Per erogare il presente servizio il fornitore dovrà disporre delle competenze, esperienze e capacità richieste ai profili professionali indicati nel seguito (per il dettaglio dei profili si rimanda all'appendice 2 Profili Professionali):

- Security Solution Architect;
- Information Security Consultant Senior;
- Information Security Consultant Junior.

Le certificazioni e le competenze richieste - e quelle eventualmente offerte- dovranno risultare aggiornate alle ultime versioni/tecnologie per tutta la durata dell'Accordo Quadro.

#### Metrica di dimensionamento e modalità di remunerazione

Per ciascuna figura professionale è prevista:

- una tariffa giornaliera "profilo base" corrispondente ad 8 ore lavorative dal lunedì al sabato dalle ore 8.00 alle ore 20.00;
- una tariffa giornaliera "profilo avanzato" corrispondente ad 8 ore lavorative dal lunedì al sabato dalle ore 20.00 alle ore 8.00, domenica e festivi.

La metrica di dimensionamento del servizio "Supporto specialistico" è: **Giorno/Persona**.

La modalità di remunerazione del servizio di "Supporto specialistico" è: **a tempo/spesa oppure a corpo**.

### 3.14 Modalità di erogazione in configurazione ibrida o on-premise

Fermo restando il modello di erogazione dei servizi definito nel Capitolato Tecnico Generale e nel presente Capitolato Tecnico Speciale, l'Amministrazione Contraente, in funzione delle proprie esigenze organizzative, delle policy interne, della tipologia di dati trattati e **in particolare per i servizi che prevedono l'impiego di tecnologie avanzate di intelligenza artificiale**, potrà richiedere che gli stessi siano erogati, in tutto o in parte, in modalità ibrida ovvero integralmente on-premise.

Tale richiesta è subordinata alla preventiva valutazione tecnica ed alla conseguente accettazione da parte del Fornitore, che ne verifica la fattibilità nell'ambito del Piano dei Fabbisogni e del Piano Operativo, nel rispetto dell'oggetto dell'Accordo Quadro e dei requisiti minimi previsti nella documentazione di gara.

In caso di accettazione, l'erogazione dei servizi nelle suddette modalità dovrà avvenire **alle medesime condizioni tecniche ed economiche previste per la modalità standard di erogazione**, fermo restando che potranno essere previste, nel Piano Operativo, specifiche declinazioni delle modalità esecutive coerenti con il contesto tecnologico e organizzativo dell'Amministrazione Contraente, senza oneri aggiuntivi a carico della stessa.

Resta altresì inteso che l'esercizio della suddetta facoltà dovrà avvenire nel rispetto delle modalità di attivazione dei servizi e dei processi di definizione del Piano dei Fabbisogni e del Piano Operativo, nonché in coerenza con i livelli di servizio e gli indicatori di qualità previsti dal presente Capitolato.

## 4 REQUISITI DI ESECUZIONE

### 4.1 ISO 9001

Ai fini dell'esecuzione dell'Accordo Quadro, il Fornitore dovrà essere in possesso di una valutazione di conformità del proprio sistema di gestione della qualità alla norma UNI EN ISO 9001, idonea, pertinente e proporzionata al seguente oggetto: **progettazione, realizzazione e/o erogazione di servizi di sicurezza**.

Il Service Desk non si considera ricompreso tra i servizi di sicurezza oggetto di certificazione.

Il possesso dovrà essere comprovato prima della stipula dell'Accordo Quadro, come previsto nel Capitolato d'Oneri.

La comprova è fornita mediante un certificato di conformità del sistema di gestione della qualità alla norma UNI EN ISO 9001.

Tale documento è rilasciato da un organismo di certificazione accreditato ai sensi della norma UNI CEI EN ISO/IEC 17021-1 per lo specifico settore e campo di applicazione/scopo del certificato richiesto, da un Ente nazionale unico di accreditamento firmatario degli accordi EA/MLA oppure autorizzato a norma dell'art. 5, par. 2 del Regolamento (CE), n. 765/2008.

In caso di raggruppamenti temporanei, consorzi ordinari, aggregazioni di imprese di rete, GEIE, il requisito dovrà essere posseduto da ogni impresa costituente il RTI o il Consorzio che svolgerà l'attività oggetto della certificazione.

In caso di consorzi di cooperative e di imprese artigiane e i consorzi stabili il requisito dovrà essere posseduto dal Consorzio e/o dalle imprese indicate quali esecutrici che svolgerà/anno l'attività oggetto della certificazione.

Il mancato possesso del suddetto requisito non consente la stipula dell'Accordo Quadro.

Il requisito dovrà essere posseduto anche dall'eventuale subappaltatore che svolgerà l'attività oggetto della certificazione.

Il requisito dovrà essere mantenuto per tutta la durata del Accordo Quadro e dei singoli Contratti Esecutivi. Nel caso in cui venga ritirata o non rinnovata la certificazione per un periodo superiore ai 3 (tre) mesi, potrà trovare applicazione apposita condizione risolutiva, come meglio indicato nell'Accordo Quadro.

### 4.2 ISO 27001

Ai fini dell'esecuzione dell'Accordo Quadro, il Fornitore dovrà essere in possesso di 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 Sicurezza e/o, Cloud e/o Sicurezza delle Informazioni**.

Il Service Desk non si considera ricompreso tra i servizi di sicurezza oggetto di certificazione.

Il possesso dovrà essere comprovato prima della stipula dell'Accordo Quadro, come previsto nel Capitolato d'Oneri.

La comprova è fornita mediante un certificato di conformità del sistema di gestione alla norma UNI EN ISO 27001.

Tale documento deve essere rilasciato da un organismo di certificazione accreditato ai sensi della norma UNI CEI ENISO/IEC 17021-1 per lo specifico settore e campo di applicazione richiesto, da un Ente nazionale unico di accreditamento firmatario degli accordi EA/MLA oppure autorizzato a norma dell'art. 5, paragrafo 2 del Regolamento (CE) n. 765/2008.

In caso di raggruppamenti temporanei, consorzi ordinari, aggregazioni di imprese di rete, GEIE, il requisito dovrà essere posseduto da ogni impresa costituente il RTI o il Consorzio che svolgerà i servizi Managed Security Services (con esclusione quindi dei servizi di supporto specialistico).

In caso di consorzi di cooperative e di imprese artigiane e i consorzi stabili il requisito dovrà essere posseduto dal Consorzio e/o dalle imprese indicate quali esecutrici che svolgerà/anno i servizi Managed Security Services (con esclusione quindi dei servizi di supporto specialistico).

Il mancato possesso del suddetto requisito non consente la stipula dell'Accordo Quadro.

Il requisito dovrà essere posseduto anche dall'eventuale subappaltatore che svolgerà l'attività oggetto della certificazione.

Il requisito dovrà essere mantenuto per tutta la durata del Accordo Quadro e dei singoli Contratti Esecutivi. Nel caso in cui venga ritirata o non rinnovata la certificazione per un periodo superiore ai 3 (tre) mesi, potrà trovare applicazione apposita condizione risolutiva, come meglio indicato nell'Accordo Quadro.

### **4.3 ISO 14001**

Ai fini dell'esecuzione dell'Accordo Quadro, il Fornitore dovrà essere in possesso di una valutazione di conformità del sistema di gestione ambientale alla norma UNI EN ISO 14001.

Il possesso dovrà essere comprovato prima della stipula dell'Accordo Quadro, come previsto nel Capitolato d'Oneri.

La comprova è fornita mediante un certificato di conformità del sistema di gestione alla norma UNI EN ISO 14001.

Tale documento deve essere rilasciato da un organismo di certificazione accreditato ai sensi della norma UNI CEI ENISO/IEC 17021-1 per lo specifico settore e campo di applicazione richiesto, da un Ente nazionale unico di accreditamento firmatario degli accordi EA/MLA oppure autorizzato a norma dell'art. 5, paragrafo 2 del Regolamento (CE) n. 765/2008.

In caso di raggruppamenti temporanei, consorzi ordinari, aggregazioni di imprese di rete, GEIE, il requisito dovrà essere posseduto da ogni impresa costituente il RTI o il Consorzio che rende disponibile il Centro Servizi.

In caso di consorzi di cooperative e di imprese artigiane e i consorzi stabili il requisito dovrà essere posseduto dal Consorzio e/o dalle imprese indicate quali esecutrici che rende/rendono disponibile il Centro Servizi.

Prima della stipula dell'Accordo Quadro dovranno essere indicate le imprese componenti del RTI/ConSORZiate esecutrici che intendono mettere a disposizione il Centro Servizi. Tali imprese potranno variare (tra quelle componenti del RTI/consorziate esecutrici) in corso di esecuzione dell'Accordo Quadro e dei Contratti Esecutivi, fermo restando che dovranno essere garantiti requisiti, nell'organizzazione del Centro Servizi, equivalenti o superiori rispetto a quelli minimi e a quelli eventualmente indicati in offerta tecnica. In tal caso la modifica dovrà essere tempestivamente comunicata a Consip S.p.A. a Consip S.p.A. o direttamente all'Organismo di coordinamento e controllo, con le modalità di cui al paragrafo 12.4 del Capitolato Tecnico Generale, e potrà diventare operativa solamente a seguito di apposita approvazione da parte dell'Organismo di coordinamento e controllo, che opererà con le modalità di cui al paragrafo 12.4 del Capitolato Tecnico Generale.

Il requisito dovrà essere posseduto anche dall'eventuale subappaltatore che eventualmente contribuirà alla messa a disposizione del Centro Servizi.

Il requisito dovrà essere mantenuto per tutta la durata del Accordo Quadro e dei singoli Contratti Esecutivi.

In particolare:

- qualora in corso di esecuzione, in caso di RTI/ConSORZI, imprese componenti/consorziate esecutrici, o imprese subappaltatrici, diverse da quelle che in sede di offerta abbiano dichiarato di mettere a disposizione il proprio Centro Servizi, intendano mettere a loro volta a disposizione il proprio Centro Servizi, il Fornitore dovrà dimostrare il possesso, da parte delle stesse, della valutazione di conformità di cui al presente paragrafo;
- qualora, in caso di RTI/ConSORZI, in corso di esecuzione un'impresa componente/consorziate esecutrice perda la valutazione di conformità di cui al presente paragrafo, la stessa non potrà più mettere a disposizione il proprio Centro Servizi, fermo restando che le prestazioni di cui al successivo capitolo 5 e relativi sottoparagrafi dovranno comunque essere garantite dal RTI/ConSORZIO mediante altre imprese/consorziate esecutrici (e/o subappaltatrici), nel rispetto dell'organizzazione del Centro Servizi risultante dall'offerta tecnica.

In ogni caso il Centro Servizi dovrà essere messo a disposizione da imprese in possesso della valutazione di conformità di cui al presente paragrafo, con la conseguenza che:

- il mancato possesso della stessa, riscontrato prima della stipula in capo a imprese che abbiano indicato di mettere a disposizione il Centro Servizi, non consente la stipula dell'Accordo Quadro;
- il mancato possesso (per tale intendendosi anche il caso in cui venga ritirata o non rinnovata) della stessa, riscontrato in corso di esecuzione dell'Accordo Quadro e dei singoli Contratti Esecutivi, per un periodo superiore a 3 mesi, in capo a imprese che mettono a disposizione

il Centro Servizi potrà comportare l'applicazione di apposita condizione risolutiva, come meglio indicato nell'Accordo Quadro.

#### 4.4 DNSH

I centri dati e le sale server utilizzati per l'erogazione dei servizi oggetto del presente Accordo Quadro dovranno essere in possesso dei requisiti "ex ante" richiesti dalla Scheda n. 8 della circolare RGS n. 22 del 14 maggio 2024, anche come eventualmente successivamente modificata.

Qualora il Fornitore abbia indicato in sede di Offerta Tecnica di usare soluzioni cloud per l'erogazione delle prestazioni oggetto del presente Accordo Quadro, gli stessi dovranno essere in possesso dei requisiti "ex ante" richiesti dalla Scheda n. 6 della circolare RGS n. 22 del 14 maggio 2024, anche come eventualmente successivamente modificata.

Prima della stipula dell'Accordo Quadro, con le modalità indicate nel Capitolato d'Oneri, Consip S.p.A. verificherà il possesso dei suddetti requisiti.

Il mancato possesso dei suddetti requisiti non consentirà la stipula dell'Accordo Quadro e gli stessi dovranno essere mantenuti per tutta la durata dell'Accordo Quadro e dei Contratti Esecutivi.

Resta inteso che, tanto prima della stipula dell'Accordo Quadro, tanto in corso di esecuzione, in caso di mancanza/perdita dei suddetti requisiti:

- a) il fornitore potrà, proporre, senza oneri aggiuntivi per la PA, l'utilizzo di centri dati e sale server diversi, ma comunque con funzionalità equivalenti o superiori rispetto a quelle eventualmente indicate in offerta tecnica e comunque in possesso dei requisiti richiesti nel presente documento. Qualora la sostituzione sia proposta in corso di esecuzione contrattuale, trova applicazione quanto previsto al paragrafo 12.4 del Capitolato Tecnico Generale;
- b) qualora non risulti percorribile l'opzione di cui al precedente punto, potrà trovare applicazione apposita condizione risolutiva, come meglio indicato nell'Accordo Quadro;

Consip S.p.A., ove richiesto dalle Amministrazioni, metterà a disposizione delle stesse i documenti acquisiti nel corso della suddetta verifica. Resta inteso che:

- è demandata alle singole Amministrazioni la responsabilità di richiedere e verificare gli ulteriori documenti necessari alla comprova dei requisiti "ex post" ovvero attinenti alla corretta esecuzione delle obbligazioni contrattuali;
- sarà altresì onere delle stesse Amministrazioni la corretta archiviazione di tutta la documentazione ai fini delle successive azioni da parte degli organi di controllo nazionali ed europei (es. audit della Commissione UE).

Il Fornitore si impegna in ogni caso a rispettare i suddetti requisiti per tutta la durata del presente Accordo Quadro e dei singoli Contratti Esecutivi fornendo la documentazione a comprova del possesso nel rispetto delle tempistiche indicate da Consip e/o dalle Amministrazioni.

#### **4.5 Info-sharing con l’Agenzia Nazionale per la Cyber sicurezza**

Ai sensi dell’art 17 del Decreto Legislativo 4 settembre 2024, n. 138 “*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersecurity nell’Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*” che promuove, lo scambio, su base volontaria, di pertinenti informazioni sulla sicurezza informatica, comprese informazioni relative a minacce informatiche, quasi-incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di sicurezza informatica e raccomandazioni concernenti la configurazione degli strumenti di sicurezza informatica per individuare le minacce informatiche, il fornitore è chiamato ad interoperare con ACN mediante la condivisione di informazioni.

L’information sharing, attraverso la condivisione di informazioni che generano una base comune di dati e conoscenza, può supportare le diverse realtà organizzative nella prevenzione, identificazione e mitigazione delle minacce, così come la gestione complessiva della postura cyber delle organizzazioni. Nel tempo, sono state sviluppate diverse modalità e piattaforme di condivisione che operano a diversi livelli; possiamo trovare esempi di reti di condivisione, ad esempio, nei seguenti ambiti:

- security operations center (soc) – con lo scopo di scambiare dati relativi agli eventi monitorati dalle organizzazioni che fanno parte della rete;
- information sharing and analysis centre (isac) – con lo scopo di scambiare dati relativi a rischi cyber, per esempio in ambito settoriale e in relazione all’interesse generale della community cyber;
- computer security incident response team (csirt) – con lo scopo di scambiare i dati relativi agli incidenti di cibersecurity raccolti dalle organizzazioni.

A tale scopo:

- il fornitore è chiamato a partecipare, mediante iscrizione, ai programmi di Info-sharing promossi da ACN, tra i quali si indica il MISP, ovvero una piattaforma usata principalmente per lo *scambio delle informazioni, arricchimento e correlazione dei dati esterni*. Questa piattaforma usa STIX/TAXII solo per lo scambio delle informazioni immagazzinate in formato JSON proprietario ed è usata normalmente come storage di dati e correlazione di IoCs (Indicatori di compromissione) da parte delle Pubbliche Amministrazioni per lo scambio di IoCs e link con le altre agenzie Europee.

- Il fornitore è chiamato a fornire periodicamente all'ACN dati aggregati sugli eventi di sicurezza monitorati in linea con la tassonomia cyber definita dall'ACN per fini statistici e di reportistica.

## 5 CENTRI SERVIZI

L'erogazione dei servizi Managed Security Services oggetto del presente Capitolato, richiede che il Fornitore dovrà disporre obbligatoriamente di uno o più Centri Servizi attivi 24H, 7 giorni su 7, 365 giorni l'anno. L'utilizzo del centro servizi non comporta alcun onere aggiuntivo per le Amministrazioni stesse.

Il Centro Servizi è inteso come la struttura complessiva all'interno della quale è ritagliata l'infrastruttura dedicata alle Amministrazioni beneficiarie dei servizi oggetto del Lotto. Il personale ad esso addetto potrà non essere esclusivamente dedicato alla erogazione dei servizi di cui al presente Capitolato ma dovranno, comunque, rispettarne i requisiti.

I Centri Servizi dovranno essere obbligatoriamente dislocati su sedi ubicate sul territorio comunitario. È fatto obbligo al Fornitore di trattare, trasferire e conservare le eventuali repliche di dati conservati dai suddetti Centri Servizi, ove autorizzate dalle Amministrazioni, sempre all'interno del territorio comunitario. Tali repliche dei dati dovranno essere conservate con livelli di sicurezza concordati con le Amministrazioni richiedenti.

La lingua di riferimento per l'erogazione dei servizi deve essere l'italiano.

Si precisa che per l'erogazione dei servizi Managed Security Services sarà possibile proporre soluzioni fruibili in modalità cloud implementate su infrastrutture distribuite anche distinte dai data center del Centro Servizi del Fornitore. In tal caso al fornitore è fatto obbligo del rispetto dei requisiti previsti al capitolo 12 e relativi sottoparagrafi del Capitolato Tecnico Generale.

Il Fornitore dovrà indicare in Offerta tecnica l'ubicazione dei Centri Servizi e le principali caratteristiche in termini di logistica e condizioni ambientali (es. almeno: infrastrutture di collegamento, impianto elettrico, dislocazione apparecchiature di rete e server, illuminazione, sicurezza, insonorizzazione, aerazione e impianto di climatizzazione artificiale). L'infrastruttura tecnologica dei Centri Servizi dovrà garantire elevati livelli di integrazione, scalabilità, performance e resilienza.

I Centri Servizi dovranno garantire la continuità per ciascun servizio erogato in remoto, in coerenza con gli orari di servizio della fornitura e con gli Indicatori di Qualità. In caso di eventi di disastro che rendono indisponibile l'intero sito preposto all'erogazione dei servizi di sicurezza, il Fornitore dovrà darne comunicazione formale ad ACN, AgID e Consip e garantire la ripartenza di tutti i servizi, anche su un diverso sito.

I Centri Servizi dovranno essere interconnessi sia alla rete Internet che alla rete SPC (profilo infranet).

Il Fornitore dovrà garantire l'interconnessione alla rete SPC tenendo conto delle possibili future evoluzioni del Sistema Pubblico di Connettività.

Alla data di pubblicazione della presente iniziativa è operativa l'infrastruttura di rete SPC (SPC2) il cui termine di scadenza contrattuale è fissato al 31/12/2026, nelle more della attivazione della nuova gara **Connettività SPC ed. 3** (SPC3) che ha ad oggetto i *servizi di connettività wired e wireless, servizi di telefonia fissa, servizi di sicurezza e servizi di supporto specialistico nell'ambito del Sistema Pubblico di Connettività (SPC)*.

Alla stipula dell'Accordo quadro, sono ipotizzabili i seguenti scenari di interconnessione alla rete SPC:

- 1) per il tramite di uno dei Fornitori aggiudicatari della suddetta gara **Connettività SPC ed. 3**;
- 2) ove la suddetta gara **Connettività SPC ed. 3** non sia ancora disponibile, per il tramite di uno dei fornitori della gara SPC2, per un periodo transitorio che si conclude con la migrazione ad un fornitore di cui al punto 1;

Successivamente alla stipula del presente Accordo quadro, il Fornitore potrà concordare con Consip una roadmap relativa alla pianificazione delle fasi di transitorio (interconnessione alla rete SPC2) e di migrazione della interconnessione alla rete SPC3.

Le interconnessioni dei Centri Servizi con la rete SPC e con la rete Internet, per l'erogazione dei servizi contrattualizzati, sono a carico dell'Aggiudicatario. Il dimensionamento delle interconnessioni dovrà essere effettuato nel rispetto dei Livelli di Servizio che il Fornitore dovrà garantire nei confronti delle Amministrazioni sottoscrittrici dei contratti esecutivi.

Per le singole Amministrazioni non è previsto alcun onere aggiuntivo per la predisposizione e l'utilizzo della connessione telematica nell'ambito di ogni servizio.

L'infrastruttura proposta dal Fornitore dovrà disporre di un proprio Autonomous System (AS) e proprie classi di indirizzamento IP pubblico (IPv4/IPv6).

Il fornitore dovrà farsi carico, qualora richiesto dall'Amministrazione, della pubblicazione dei servizi tramite un Servizio DNS.

E' responsabilità del Fornitore assicurare che i Centri Servizi, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni da e verso la rete SPC nel rispetto delle regole tecniche di interconnessione (o eventuali future infrastrutture di rete che dovessero essere rese disponibili alla PA) e verso la rete Internet siano protette mediante l'adozione di sistemi e metodologie, nel rispetto di quanto stabilito dallo standard ISO/IEC 27001, oltre che gestite in piena conformità con la normativa vigente.

L'interconnessione alla rete Internet dovrà avvenire per il tramite di almeno due differenti Service Provider afferenti a due POP con cammini distinti.

Le modalità di attuazione dei requisiti di sicurezza del Centro Servizi dovranno essere dettagliate all'interno dei seguenti documenti:

- **Sistema di Gestione della Sicurezza delle Informazioni (ISMS)**, consistente in un processo iterativo articolato in successive implementazioni, monitoraggi e successive fasi di riesame e miglioramento.
- **Piano della Sicurezza dei Centri Servizi**, che dovrà descrivere approfonditamente le modalità logistiche ed organizzative, gli strumenti ed i sistemi che il Fornitore intende adottare o di cui è provvisto per rendere sicuro e protetto l'ambiente in cui sono ospitati le infrastrutture, il software e i dati delle Amministrazioni.

Il Fornitore Aggiudicatario dovrà garantire la disponibilità dei documenti sopra elencati nei tempi di seguito indicati, Tali documenti potranno essere oggetto di osservazioni e richieste di aggiornamento da parte di Consip.

Nome documento	Contenuti previsti	Data di disponibilità
Sistema di Gestione della Sicurezza delle Informazioni (ISMS)	§5.1	Prima consegna alla stipula dell'Accordo Quadro; successivi aggiornamenti entro 30 gg lavorativi dalla richiesta
Piano di Sicurezza del Centro Servizi	§5.2	Prima consegna alla stipula dell'Accordo Quadro; successivi aggiornamenti entro 30 gg lavorativi dalla richiesta

*Tabella 2 – Date di disponibilità dei documenti*

Consip si riserva la possibilità di eseguire un collaudo dei Centri Servizi secondo le modalità esplicitate nel Capitolo 9 del Capitolato Tecnico Generale.

## **5.1 Sistema di Gestione della Sicurezza delle Informazioni (ISMS)**

Il Fornitore dovrà prevedere per il Centro Servizi l'instaurazione di un adeguato sistema di gestione della sicurezza delle informazioni (ISMS), consistente in un processo iterativo articolato in successive implementazioni, monitoraggi e successive fasi di riesame e miglioramento.

Il perimetro di validità del ISMS è quello individuato dai dati gestiti dal Sistema Informativo e dalle risorse e strumenti ad essi afferenti gestiti dal Fornitore relativamente all'erogazione dei servizi oggetto di fornitura.

Il Fornitore dovrà implementare il proprio ISMS in relazione alle specifiche espresse nel presente documento e in considerazione degli standard e della normativa di riferimento, di cui i principali riferimenti sono riportati al paragrafo 2.2 del Capitolato Tecnico Generale.

Consip si riserva la facoltà di richiedere durante la durata del contratto la documentazione di attuazione del ISMS prodotta dal Fornitore, il quale dovrà consegnarla entro 30 solari giorni dalla richiesta; tale documentazione dovrà essere mantenuta costantemente aggiornata in relazione alle successive evoluzioni del sistema.

Per tale documentazione il Fornitore dovrà definire e implementare una procedura che definisca le azioni di gestione necessarie a:

- riesaminare ed aggiornare i documenti e riapprovare i documenti in caso di modifiche successive;
- assicurarsi che siano identificati i cambiamenti e l'attuale stato di revisione dei documenti;
- assicurarsi che le versioni più recenti dei documenti rilevanti siano facilmente identificabili e disponibili prevenendo l'utilizzo non intenzionale di documenti obsoleti.

Il Fornitore dovrà predisporre strumenti e processi di gestione della documentazione opportuni al fine di garantire la conservazione e l'aggiornamento della documentazione di sistema.

Nell'implementazione dell'ISMS il Fornitore dovrà rendere disponibili i seguenti deliverable:

Deliverable	Descrizione	Data di disponibilità
Documento di gestione delle registrazioni	Definire e mantenere le registrazioni che forniscono evidenza della conformità ai requisiti e dell'efficace operatività del ISMS (es.: libro dei visitatori, le registrazioni degli audit e l'autorizzazione per gli accessi fisici e logici, ecc.)	Entro 20 giorni solari dalla richiesta di Consip
Programma e procedura Audit	Predisposizione procedura e conduzione di audit interni sul proprio ISMS ad intervalli pianificati, con cadenza almeno annuale, al fine di determinare se gli obiettivi del controllo, i controlli, i processi e le procedure del ISMS	Entro 20 giorni solari dalla stipula dell'Accordo Quadro e entro 20 giorni solari da ogni successivo aggiornamento
Template campi del Registro delle azioni	Predisporre il Registro delle azioni per la registrazione di ogni incidente e/o rilievo (derivante da visite ispettive di Consip, da audit interni o da segnalazione spontanee) ove indicare le azioni da intraprendere per eliminare la causa dei rilievi e degli incidenti allo scopo di prevenirne	Entro 20 giorni solari dalla stipula dell'Accordo Quadro e entro 20 giorni solari da ogni

Deliverable	Descrizione	Data di disponibilità
	la reiterazione coerentemente con la procedura documentata di audit, da presentare a Consip su richiesta.	successivo aggiornamento
Piano di Incident Response (IRP)	Predisporre un documento che raccoglie informazioni e procedure utili ad affrontare le situazioni di emergenza provocate da un'ampia gamma di attacchi alla sicurezza informatica di un'azienda: ransomware, malware, phishing, attacchi DDoS, intrusioni nella rete, oltre alle vulnerabilità delle applicazioni e alle minacce interne, come gli errori dei dipendenti o i tentativi di sabotaggio. In altri termini, il principale obiettivo del piano di incident response risiede nel rilevare, rispondere e limitare i danni derivanti dagli attacchi alla sicurezza informatica dell'azienda. Il documento, ed ogni suo successivo aggiornamento, sarà consegnato a Consip su richiesta.	Entro 20 giorni solari dalla stipula dell'Accordo Quadro e entro 20 giorni solari da ogni successivo aggiornamento
Piano di formazione cyber	Predisporre il piano di formazione per lo svolgimento di sessioni formative per il personale in materia di cybersecurity o la predisposizione di test periodici volti a verificare la sicurezza dell'infrastruttura IT e l'efficacia delle misure implementate.	Entro 20 giorni solari dalla stipula dell'Accordo Quadro e entro 20 giorni solari da ogni successivo aggiornamento
Template per il Riesame del ISMS	Esecuzione, con cadenza almeno annuale, del riesame sulle Politiche della Sicurezza delle Informazioni includendo la valutazione delle opportunità per il miglioramento e la necessità di cambiamenti del ISMS. I risultati del riesame sono documentati all'interno di un'apposita Relazione di riesame del Fornitore. Consip si riserva di effettuare controlli in un qualsiasi momento.	Entro 20 giorni solari dalla richiesta di Consip.
Valutazione dei rischi	Predisporre un documento, con aggiornamento almeno annuale, contenente la valutazione dei rischi inerenti ai Centri Servizi e la sicurezza delle informazioni gestite. Il documento, ed ogni suo	Entro 20 giorni solari dalla stipula dell'Accordo Quadro e entro 20 giorni

Deliverable	Descrizione	Data di disponibilità
	successivo aggiornamento, sarà consegnato a Consip su richiesta.	solari da ogni successivo aggiornamento
Modulo di reporting per le analisi periodiche di Incidenti, Criticità e Malfunzionamenti	Predisporre documento di registrazione, degli incidenti rilevati dal proprio personale o da strumenti di monitoraggio a disposizione dei vari servizi della fornitura. Ogni situazione anomala dovrà essere registrata e segnalata alle Amministrazioni interessate dai servizi forniti e, laddove necessario, a Consip, con gli strumenti definiti nelle apposite procedure di gestione. Il registro degli incidenti costituirà anche la base per la raccolta delle evidenze necessarie in caso di procedimenti disciplinari e legali. Il documento, ed ogni suo successivo aggiornamento, sarà consegnato a Consip su richiesta.	Entro 20 giorni solari dalla stipula dell'Accordo Quadro e entro 20 giorni solari da ogni successivo aggiornamento

*Tabella 3 – Elenco deliverable*

## 5.2 Piano di sicurezza dei Centri Servizi

Il Piano di Sicurezza dovrà descrivere approfonditamente le modalità logistiche ed organizzative, gli strumenti e i sistemi che il Fornitore intende adottare o di cui è provvisto per rendere sicuro e protetto l'ambiente da cui avviene l'erogazione dei servizi e in cui sono ospitati i dati dell'Amministrazione. Consip si riserva la possibilità di richiedere, nel corso della fornitura, le variazioni ritenute opportune al Piano della Sicurezza dei Centri Servizi predisposto dall'Aggiudicatario.

Il Piano di sicurezza dovrà essere formulato in coerenza con la ISO 27001.

Consip si riserva la facoltà di richiedere, ogni volta che lo reputino opportuno, una nuova versione o revisione del Piano della Sicurezza del Centro Servizi e della documentazione comprovante la corretta esecuzione delle procedure ed istruzioni previste dal Piano della Sicurezza dei Centri Servizi.

Il Piano della sicurezza dovrà:

- illustrare la propria organizzazione che sarà chiamata ad interagire con l'Amministrazione;
- illustrare le modalità con cui garantire la sicurezza delle informazioni gestite e delle strutture di elaborazione delle informazioni, elaborate, comunicate e/o gestite da terze parti esterni;
- identificare i rischi per le informazioni dell'Amministrazione e per le strutture di elaborazione delle informazioni, derivanti da processi che coinvolgono parti esterne e realizzare gli

- appropriati controlli al perimetro prima di consentire gli accessi fisici (a uffici, stanze con computer, archivi, ecc) e logici (ambienti software, database, ecc);
- identificare tutti gli asset dedicati alla fornitura e da gestire, compilando e tenendo aggiornato un inventario di tali asset, da allegare al Piano della Sicurezza;
  - illustrare le modalità con cui conseguire e mantenere attiva un'adeguata protezione degli asset utilizzati per l'erogazione dei servizi forniti;
  - illustrare le linee guida per la classificazione delle informazioni dell'Amministrazione trattate rispetto al loro valore, alle prescrizioni legali, alla sensibilità ed alla criticità. Tali linee guida dovranno contenere i criteri di individuazione delle informazioni che sono da considerarsi sensibili o critiche per le Amministrazioni;
  - illustrare le modalità di informazione e formazione del personale coinvolto nell'erogazione dei servizi oggetto della presente fornitura. Tutte le persone fisiche e giuridiche che hanno un ruolo nella gestione della sicurezza delle informazioni (Responsabili e Incaricati al trattamento delle informazioni delle Amministrazioni e del Fornitore) all'interno della struttura del Fornitore, dovranno essere informate e formate sulle responsabilità associate a detto ruolo, sulle modalità di gestione delle informazioni e sull'utilizzo degli impianti elettronici, dei sistemi informativi, dei servizi cui essi hanno accesso e sulle relative politiche di sicurezza;
  - illustrare le modalità con cui predisporre strumenti, processi di gestione e documentazione opportuni a supporto:
    - della identificazione e gestione delle aree sicure (il perimetro di sicurezza fisica di sua competenza. Un perimetro di sicurezza è costituito da una barriera, come un muro, un cancello d'ingresso, un tornello controllato da tessere o una reception);
    - della prevenzione della perdita, danneggiamento, furto o compromissione di asset e l'interruzione delle attività organizzative presenti, dando evidenza delle misure adottate necessarie per minimizzare i danni derivanti da: furto, incendio, esplosione, fumo, allagamento, ammanchi di erogazione d'acqua, polveri, vibrazioni, effetti chimici, interferenze nell'erogazione di corrente, radiazioni elettromagnetiche anche derivanti da edifici adiacenti.
    - delle procedure operative e degli strumenti a supporto atte a garantire i servizi oggetti di fornitura. Tali procedure dovranno almeno includere:
      - gestione di servizi di terze parti;
      - protezione contro software dannosi e codici auto eseguibili;
      - backup e restore;
      - disaster recovery;
      - gestione della sicurezza di rete;
      - trattamento dei supporti rimovibili;
      - trasmissione delle informazioni;
      - monitoraggio degli accessi e dell'uso dei sistemi;

- log di audit;
- protezione dei log;
- log degli amministratori e degli operatori;
- log degli errori.
- degli strumenti, processi di gestione e documentazione opportuni a supporto del controllo degli accessi logici controllati attraverso processi formali di registrazione e de-registrazione dell'utente;
- delle procedure di gestione degli incidenti di sicurezza;
- del processo per lo sviluppo ed il mantenimento della continuità operativa per i processi e sistemi critici; il processo di gestione della continuità operativa dovrà essere allineato al D.Lgs. del 26 agosto 2016 n. 179 ed alle linee guida per il disaster recovery delle Pubbliche Amministrazioni redatte da AgID.

Il Piano della sicurezza dovrà contenere il seguente deliverable:

Deliverable	Descrizione	Data di disponibilità
Politiche di sicurezza	Predisporre un documento che descriva le Politiche di Sicurezza in conformità alle norme applicabili, agli impegni presi in ambito contrattuale e nella propria offerta per la presente gara. Tale documento dovrà contenere oltre che gli obiettivi ed i principi di base, anche le regole, le procedure operative ed organizzative adottate dal Fornitore per la conduzione dei servizi previsti dal Capitolato. Il documento, ed ogni suo successivo aggiornamento, sarà consegnato a Consip su richiesta.	Entro 20 giorni solari dalla stipula dell'Accordo Quadro e entro 20 giorni solari da ogni successivo aggiornamento

## 6 ADEMPIMENTI A CARICO DEL FORNITORE

### 6.1 SERVICE-DESK

Il Fornitore dovrà rendere disponibile un Service Desk, attivo 24H, 7 giorni su 7, 365 giorni l'anno, dedicato all'assistenza in remoto, che abbia almeno le caratteristiche minime di seguito indicate.

L'utilizzo del Service Desk non comporta alcun onere aggiuntivo per le Amministrazioni stesse.

Il servizio di assistenza in remoto è rivolto ai Referenti tecnici identificati dalle Amministrazioni e dovrà fornire un punto di accesso unificato e un insieme di funzioni di assistenza.

Tale assistenza dovrà gestire almeno:

- gli aspetti amministrativi e contrattuali relativi ai Contratti Esecutivi anche per ciò che riguarda le fasi e attività propedeutiche alla stipula degli stessi; in tal caso, gli utenti target del servizio saranno i Referenti delle Amministrazioni, incaricati della gestione degli aspetti amministrativi in ambito;
- la segnalazione e tracciamento degli incidenti di sicurezza da parte dell'Amministrazione o dal Fornitore; i Referenti tecnici delle Amministrazioni fungeranno da interlocutori con le strutture del Service Desk, gestendo al proprio interno il contatto con gli utenti dei servizi;
- le segnalazioni e tracciamento di malfunzioni relative ai servizi oggetto della fornitura da parte dell'Amministrazione o dal Fornitore; i Referenti tecnici delle Amministrazioni fungeranno da interlocutori con le strutture del Service Desk, gestendo al proprio interno il contatto con gli utenti dei servizi.

Alla stipula del Contratto esecutivo, le Amministrazioni contraenti renderanno disponibili al Fornitore le informazioni necessarie (es. lista dei referenti) e, ove disponibile, il numero medio di contatti ipotizzabili nel periodo di riferimento.

Il Fornitore dovrà strutturare il servizio di assistenza in remoto in modo da presentare un'interfaccia unica verso gli utenti ed assicurare la tracciabilità in termini di segnalazioni/azioni intraprese. In particolare, dovrà essere reso disponibile:

- un servizio di help desk telefonico, accessibile attraverso chiamata su un unico numero verde in tempo reale e con un tempo di attesa in coda come da specifico Indicatore di Qualità;
- un servizio di supporto via e-mail, integrato con il sistema di Trouble Ticketing;
- un'interfaccia web che consenta al referente tecnico dell'Amministrazione di inoltrare segnalazioni attraverso il sistema di Trouble Ticketing e di seguire il ciclo di vita.

Il Fornitore dovrà rendere disponibile un "Sistema di Trouble Ticketing (TT)" per:

- la gestione dei trouble ticket aperti proattivamente dal Fornitore stesso;
- la gestione dei trouble ticket aperti dalle Amministrazioni beneficiarie;
- la gestione della riassegnazione di trouble ticket a strutture tecniche di secondo livello;
- il monitoraggio dello stato di avanzamento dei trouble ticket aperti.

La registrazione delle segnalazioni di malfunzionamento e delle richieste di servizio dovrà avvenire attraverso l'utilizzo del sistema di trouble ticket che dovrà tracciare almeno le informazioni minime seguenti:

- codice identificativo del trouble ticket;
- descrizione della segnalazione (malfunzionamento, richiesta di servizio);
- modalità di ricezione (telefono, internet, etc.);
- data e orario di apertura;
- soggetto che ha richiesto l'intervento;
- elenco e numero di elementi complessivamente coinvolti dal malfunzionamento;
- classificazione della segnalazione (priorità, severità, etc);
- riferimenti operativi coinvolti nel caso specifico;
- smistamento al secondo livello qualora non fosse possibile fornire la soluzione;
- stato del trouble ticket;
- descrizione della soluzione;
- diagnosi del malfunzionamento, ove applicabile;
- data e orario di chiusura.

## **6.2 GESTIONE DEGLI INCIDENTI DI SICUREZZA**

Il processo di gestione degli incidenti di sicurezza si applica a tutti gli incidenti di natura cyber, indipendentemente dal dominio di origine, comprendendo:

- a) gli incidenti che interessano direttamente sistemi, dati o servizi dell'Amministrazione;
- b) gli incidenti che originano o si verificano nei sistemi, nelle infrastrutture, nei Centri Servizi o nella catena di fornitura del Fornitore, qualora tali eventi possano, anche potenzialmente, impattare sulla sicurezza, disponibilità o integrità dei servizi erogati all'Amministrazione.

In fase di erogazione il Fornitore, al verificarsi di incidenti di sicurezza, dovrà garantire l'attuazione di un processo di gestione al fine di evitare o minimizzare la compromissione dei dati e dei servizi dell'Amministrazione.

L'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, dovrà consentire il miglioramento continuo della capacità di risposta agli incidenti di sicurezza informatica.

Il Fornitore dovrà utilizzare la tassonomia cyber TC-ACN definita da ACN disponibile al link: <https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn> che consente:

- di agevolare lo scambio di informazioni a livello nazionale attraverso l'adozione di un lessico comune che rappresenti una base metodologica sia per la condivisione di informazioni riguardo agli eventi cyber sia per la notifica degli incidenti al CSIRT Italia;

- di identificare, definire e caratterizzare gli eventi cyber attraverso un'unica tassonomia rilevante a livello nazionale;
- di fornire alle organizzazioni un documento da armonizzarsi con le tassonomie internazionali in materia di cybersecurity e che sia al contempo adeguato al contesto normativo nazionale.

Il processo di gestione degli incidenti di sicurezza dovrà inoltre consentire all'Amministrazione il rispetto degli obblighi derivanti:

- dal Decreto Legislativo 4 settembre 2024, n. 138 Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersecurity nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;
- dal Regolamento GDPR n. 679/2016 in materia di violazione di dati personali;
- da quanto indicato dal DPCM n. 81/2021 *“Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza”*;
- dalla Legge 28 giugno 2024, n. 90 recante *“Disposizioni in materia di rafforzamento della cybersecurity nazionale e di reati informatici”*;
- dalle rispettive norme e prassi attuative.

Il processo di Incident Response dovrà garantire le seguenti fasi:

- segnalazione;
- preparazione, identificazione e analisi dell'incidente;
- contenimento dei danni relativi all'incidente ed impedimento alla sua propagazione;
- raccolta e trasmissione nel modo appropriato delle evidenze digitali di reato;
- ripristino dei sistemi e delle applicazioni;
- valutazione postuma dell'incidente volta al miglioramento continuo.

### Segnalazione

Segnalazione al Service Desk da parte dell'Amministrazione di un incidente di sicurezza (inteso come un qualsiasi evento che comprometta l'integrità, la disponibilità o la riservatezza dei dati all'interno dei sistemi della organizzazione) e/o generata in automatico dagli strumenti di monitoraggio e controllo del Fornitore.

Il Fornitore è altresì tenuto a segnalare tempestivamente al Service desk e all'Amministrazione qualsiasi incidente di sicurezza rilevato o di cui sia venuto a conoscenza che:

- interessi direttamente i sistemi, le infrastrutture o i servizi dell'Amministrazione;

- ovvero si verifichi nell'ambito dei propri sistemi, dei Centri Servizi, delle infrastrutture utilizzate per l'erogazione dei servizi o della propria catena di fornitura, qualora tale evento possa, anche potenzialmente, avere impatti sulla sicurezza, disponibilità o integrità dei servizi erogati all'Amministrazione.

#### Preparazione

In questa fase rientrano non solo le azioni propedeutiche a creare le condizioni migliori per gestire gli incidenti in maniera appropriata ma anche tutte quelle azioni da intraprendere per prevenirli. Le prime fanno riferimento principalmente alla stesura del piano di Incident Response e alla definizione delle procedure operative da parte del fornitore. Le seconde si riferiscono alla verifica della corretta configurazione dei sistemi di monitoraggio e di sicurezza dell'organizzazione.

#### Identificazione e analisi di un incidente

Si tratta di un insieme di attività che mirano a valutare se un evento riscontrato sia effettivamente riconducibile ad un incidente di sicurezza oppure si tratti di un cosiddetto "falso positivo".

Tale fase dovrà comprendere i seguenti deliverable:

**DELIVERABLE:** *Avviso di preallarme*. Prima investigazione dell'incidente da parte delle strutture tecniche del Fornitore che dovrà indicare se la segnalazione raccolta sia effettivamente riconducibile ad un incidente di sicurezza oppure si tratti di un falso positivo e dovrà prevedere la trasmissione da parte del Fornitore al referente tecnico dell'Amministrazione del deliverable *Avviso di preallarme* o pre-notifica esplicativo dei primi elementi. Tale attività dovrà essere svolta nel rispetto degli indicatori di qualità di cui all'Appendice 1 del presente capitolato e ove eventualmente migliorati in sede offerta tecnica.

**DELIVERABLE:** *Notifica dell'incidente di sicurezza*. Seconda investigazione dell'incidente da parte delle strutture tecniche del Fornitore che dovrà prevedere la trasmissione da parte del Fornitore al referente tecnico dell'Amministrazione del deliverable *Notifica dell'incidente di sicurezza* esplicativa di una valutazione dell'incidente, del livello di gravità e della natura dell'incidente di sicurezza, dell'impatto e degli eventuali indicatori di compromissione. Tale attività dovrà essere svolta nel rispetto degli indicatori di qualità di cui all'Appendice 1 del presente capitolato e ove eventualmente migliorati in sede offerta tecnica.

#### Identificazione delle azioni di contenimento relative all'incidente

Si tratta di un'attività che mira ad identificare le possibili azioni correttive che occorre da subito intraprendere per contrastare l'attacco e prevenire la sua propagazione.

Tale fase dovrà comprendere almeno le seguenti attività:

- identificazione delle azioni di contenimento di breve periodo da parte del Fornitore e successiva segnalazione all'Amministrazione degli interventi considerati essenziali ed urgenti atti a mettere in sicurezza gli eventuali sistemi interessati dall'incidente, senza inquinare eventuali evidenze digitali di reato. Se ne riportano alcune a titolo di esempio:
  - creazione di regole firewall atte a bloccare l'accesso ai sistemi coinvolti;
  - disabilitazione di account utente sui sistemi centralizzati di autenticazione;
  - cambio di configurazione sui sistemi DNS;
  - disconnessione dei sistemi coinvolti dalla rete mediante riconfigurazione di apparati di rete.
- Identificazione delle azioni di contenimento di lungo periodo, di cui se ne riportano alcune a titolo di esempio:
  - installazione di patch o aggiornamenti di sistema e/o applicativi;
  - cancellazione di file o dati;
  - arresto di servizi o processi malevoli;
  - cambio di configurazione di programmi/apparati.

#### Raccolta e trasmissione delle evidenze digitali di reato

L'attività è volta all'acquisizione di eventuali evidenze digitali (es. mediante copia forense dei dischi, esecuzione di normali backup atti a mettere in sicurezza i dati) da utilizzare nella eventuale ricostruzione di quanto accaduto in seguito all'incidente. È quindi necessario procedere all'acquisizione forense delle evidenze digitali di reato in ogni caso in cui si prevede un prosieguo in ambito legale come per esempio nei seguenti casi:

- accessi abusivi a sistemi o informazioni;
- attività illecite commesse dal personale o comunque mediante il sistema Informativo gestito dall'Amministrazione;
- interruzione di pubblici servizi critici;
- violazioni della privacy di utenti e cittadini;
- utilizzo illegale dei sistemi per perpetrare truffe o diffondere materiale illecito.

Le evidenze digitali raccolte dovranno essere trasmesse dal Fornitore al referente tecnico dell'Amministrazione e archiviate.

#### Ripristino dei sistemi e delle applicazioni

Le operazioni di ripristino dei sistemi e delle applicazioni sono volte alla rimozione ed eliminazione definitiva del problema o della vulnerabilità utilizzata per compromettere un sistema coinvolto in un incidente e riportarlo ad un livello di sicurezza elevato.

Le attività che sono solitamente eseguite in questa fase possono essere di diverso tipo, per esempio:

- aggiornamento di release dei sistemi operativi o del software presente (per rimuovere eventuali vulnerabilità di sicurezza);

- rimozione di eventuali servizi o software che, utilizzati in modo malevolo, possono compromettere il sistema stesso.

In questa fase le operazioni eseguite mirano principalmente a verificare che i sistemi coinvolti nell'incidente siano stati correttamente riattivati e che siano nuovamente sicuri, per considerare l'incidente effettivamente chiuso.

Le operazioni di ripristino verranno attuate dalle strutture gestionali dell'Amministrazione e/o del Fornitore in base alla responsabilità di amministrazione dei sistemi/servizi interessati.

**DELIVERABLE:** *Relazione stato avanzamento*: dalla notifica dell'incidente di sicurezza e fino alla sua conclusione, il Fornitore dovrà prevedere la trasmissione al referente tecnico dell'Amministrazione del deliverable *Relazione stato avanzamento* contenente una descrizione dettagliata dell'incidente, la sua gravità e il suo impatto, l'origine e le misure di attuazione in corso di adozione.

La *Relazione stato avanzamento* dovrà essere prodotta e trasmessa periodicamente all'Amministrazione con periodicità prestabilita sino alla conclusione dell'incidente e dovrà contenere un aggiornamento delle misure di attuazione che progressivamente vengono adottate.

Tale attività dovrà essere svolta nel rispetto degli indicatori di qualità di cui all'Appendice 1 del presente capitolato.

Dal punto di vista tecnico le operazioni di chiusura del ticket relativo all'incidente di sicurezza avvengono con la dichiarazione della fine dello stato di incidente da parte del referente tecnico dell'Amministrazione.

#### Valutazione a posteriori dell'incidente volta al miglioramento continuo

Successivamente alla chiusura dell'incidente il Fornitore dovrà valutare le operazioni eseguite per la gestione dello stesso, evidenziando, ove presenti, sia i punti in cui queste sono state eseguite in conformità con le procedure del proprio ISMS di cui al capitolo 5, sia le aspettative dell'Amministrazione, sia eventuali problemi sorti durante lo svolgimento delle operazioni.

Sulla base delle criticità rilevate durante l'esecuzione delle operazioni il Fornitore dovrà provvedere alla correzione, migliorando sia le proprie procedure tecniche di gestione sia la capacità di operare delle strutture preposte, agendo sulle infrastrutture e i sistemi, dandone evidenza all'Amministrazione.

Il processo di gestione degli incidenti di sicurezza dovrà essere condiviso con l'Amministrazione nell'ambito delle attività previste nella fase di presa in carico di cui al paragrafo 7.1, e potrà essere adattato, ove richiesto dall'Amministrazione, in relazione alle modalità gestionali della stessa.

**DELIVERABLE:** *Relazione finale post risoluzione*: a chiusura dell'incidente di sicurezza, il Fornitore dovrà prevedere la trasmissione al referente tecnico dell'Amministrazione del deliverable *Relazione finale post risoluzione* contenente una descrizione dettagliata dell'incidente, la sua gravità e il suo

impatto, l'origine e le misure di attuazione adottate e in corso di adozione e l'eventuale impatto transfrontaliero dell'incidente. Tale attività dovrà essere svolta nel rispetto degli indicatori di qualità di cui all'Appendice 1 del presente capitolato.

## 7 FASI OPERATIVE DELLA FORNITURA

Il Fornitore dovrà garantire l'esecuzione della fornitura attraverso il pieno rispetto dei requisiti minimi e dei livelli di servizio a partire dalla data di stipula del contratto.

In tutte le attività propedeutiche all'attivazione dei servizi, il Fornitore dovrà impiegare personale pienamente addestrato sulle tematiche tecniche e normative oggetto della fornitura nonché ampiamente formato sulle metodologie, strumenti e standard che saranno utilizzati nel corso della fornitura.

Di seguito le fasi operative della fornitura:

- a) presa in carico e startup;
- b) erogazione a regime;
- c) fine fornitura.

### 7.1 Presa in carico e startup

Dalla data di stipula dell'Accordo quadro e fino alla data di presa in carico e startup, il Fornitore dovrà predisporre i collegamenti telematici e di rete del Centro servizi per l'interconnessione alla rete SPC.

Entro il termine di 10 giorni lavorativi dalla data di stipula di ciascun Contratto esecutivo, il Fornitore dovrà elaborare e presentare il Piano di Lavoro Generale coerente con il fabbisogno, che rappresenta la totalità dei servizi richiesti e le attività propedeutiche all'attivazione dei servizi. Tale piano dovrà contenere al proprio interno anche il Piano di Presa in carico e startup.

Il Piano di Presa in carico e startup è soggetto all'approvazione dell'Amministrazione e dovrà contenere il dettaglio delle attività che devono essere espletate ad inizio contratto per l'attivazione dei servizi oggetto di fornitura; in particolare:

- predisposizione della documentazione, impegno delle risorse professionali impiegate e la pianificazione temporale;
- acquisizione del know-how del contesto tecnico e funzionale dell'Amministrazione, ove richiesto dalla stessa;
- predisposizione e configurazione dei servizi oggetto di fornitura nonché di eventuali strumenti tecnologici offerti;
- condivisione, ed eventuale adattamento e integrazione con i processi di gestione degli incidenti dell'Amministrazione;
- predisposizione della documentazione relativa alle modalità di misurazione degli Indicatori di Qualità;
- predisposizione dell'elenco delle risorse professionali ed il corrispondente impegno in termini di giornate lavorative durante la fase di presa in carico;
- indicazione del nominativo dei responsabili tecnici dei servizi;
- predisposizione del gantt dei servizi, contenente:
  - date di inizio e fine, previste ed effettive, delle singole attività;

- date di consegna, previste ed effettive, dei singoli prodotti.

La fase di presa in carico e startup è a totale carico del Fornitore e non comporterà oneri aggiuntivi per l'Amministrazione.

Si precisa che almeno il 50% delle risorse professionali impiegate dal Fornitore nelle attività di presa in carico e startup e dei referenti tecnici delle attività dovranno successivamente essere impiegati nell'erogazione dei servizi. La fase di presa in carico e startup dovrà essere completata entro il termine massimo di 30 giorni solari dalla data di approvazione del Piano da parte dell'Amministrazione, salvo diverso termine concordato con l'Amministrazione.

## 7.2 Modalità di attivazione dei servizi

Il paragrafo definisce le modalità di attivazione dei servizi di ogni Contratto Esecutivo. Il Fornitore dovrà obbligatoriamente eseguire quanto di seguito descritto sia nel caso di migrazione di un'Amministrazione da servizi preesistenti, sia nel caso di presa in carico ex novo.

In relazione ad eventuali attività di installazione (e successiva manutenzione) presso le sedi dell'Amministrazione (ad esempio installazione di appliance), il Fornitore dovrà obbligatoriamente definire, congiuntamente con l'Amministrazione contraente, il piano di installazione/manutenzione dei servizi, che dovrà rispettare i seguenti requisiti minimi:

- gli interventi dovranno essere effettuati in fasce orarie definite dall'Amministrazione, coerentemente con le proprie esigenze di operatività;
- l'operatività del servizio dovrà essere garantita anche durante la fase intermedia di test e collaudo;
- l'impatto delle operazioni di roll-out e installazione sulla normale operatività delle sedi dovrà essere ridotto all'essenziale.

Qualora un'operazione di installazione dovesse costituire causa di disservizio, il Fornitore dovrà adoperarsi per garantire il ripristino immediato della condizione preesistente (procedura di *roll-back*). A partire dalla data di decorrenza del Contratto esecutivo, il Fornitore dovrà procedere all'installazione secondo le modalità temporali previste dal Piano Operativo; per tale attività e per le eventuali successive attività di configurazione il Fornitore, congiuntamente con l'Amministrazione, dovrà:

- contattare il referente tecnico del servizio;
- concordare le modalità ed i tempi di interventi on-site;
- effettuare una verifica del sito, se necessario;
- procedere alle specifiche attività di installazione e configurazione;
- partecipare alle attività di test ed emettere un verbale congiunto per collaudo eseguito con esito positivo.

Nel caso in cui la presa in carico di un servizio richiedesse attività di migrazione, il Fornitore dovrà obbligatoriamente concordare con l'Amministrazione contraente un piano specifico, nel quale indicare obbligatoriamente gli interventi da eseguire e le relative fasce orarie. Tutti gli interventi eseguiti sulle piattaforme in esercizio dovranno obbligatoriamente essere effettuati al di fuori dell'orario di lavoro del personale delle Amministrazioni e, comunque, in intervalli orari definiti dall'Amministrazione coerentemente con le proprie esigenze di operatività.

Pur nel rispetto della continuità del servizio, il piano proposto dal Fornitore deve consentire il massimo parallelismo delle attività al fine di minimizzare i tempi di attivazione.

Il processo deve prevedere, ove applicabile, una fase di "parallelo operativo" che garantisca, in una determinata finestra temporale, la coesistenza dei servizi erogati dall'attuale Fornitore. Il parallelo operativo deve essere tenuto attivo per il tempo necessario a completare le attività di migrazione e verificare la corretta operatività dei nuovi servizi.

Le attività di migrazione verranno svolte mediante l'utilizzo del Supporto specialistico; il pagamento dei corrispettivi per la fornitura dei servizi oggetto di migrazione decorrerà dalla data di collaudo positivo (verbale di collaudo) del servizio ovvero dalla data di accettazione da parte dell'Amministrazione.

### **7.3 Fine fornitura**

Negli ultimi 60 giorni solari di validità del contratto, il Fornitore dovrà svolgere, sulla base di un Piano di Trasferimento, le attività di passaggio di consegne di fine fornitura con il trasferimento all'Amministrazione o a terzi da essa indicati, del know-how e delle competenze maturate nella conduzione dei servizi oggetto del Contratto esecutivo.

Il Piano di Trasferimento dovrà essere elaborato dal Fornitore e sottoposto all'approvazione dell'Amministrazione nei 30 giorni solari antecedenti lo svolgimento delle attività di passaggio di consegne.

Tale fase, consiste nelle seguenti attività da considerarsi come requisiti minimi:

- trasferimento del Know-how relativo al contesto dei servizi erogati alla Amministrazione;
- consegna dei dati dell'Amministrazione;
- consegna della documentazione tecnica completa e aggiornata allo stato dell'arte dei servizi.

Il passaggio di consegne di fine fornitura dovrà essere erogato dal Fornitore nel corso dell'ultimo mese di vigenza contrattuale del Contratto esecutivo, secondo la pianificazione concordata, senza alcun onere per l'Amministrazione.

Il Fornitore dovrà mettere a disposizione un apposito gruppo di lavoro dedicato, con un numero adeguato di risorse professionali, strumenti organizzativi e tecnologici, anche in relazione a quanto ulteriormente richiesto dall'Amministrazione.

Sono incluse nelle attività di trasferimento:

- il supporto all'Amministrazione nella definizione della progettazione di dettaglio delle attività (predisposizione Piano di trasferimento, revisione documenti, ecc.);
- lo svolgimento delle attività di propria pertinenza in conformità alla pianificazione definita;
- il coordinamento generale e la supervisione delle attività di trasferimento di tutti gli attori coinvolti;
- il supporto e il monitoraggio continuativo, per tutta la durata delle attività di trasferimento, a tutti gli attori coinvolti per lo svolgimento delle attività;
- il reporting delle attività svolte al termine del trasferimento.

Di seguito si riportano i vincoli previsti nell'ambito del trasferimento:

- durata massima delle attività di trasferimento: 30 giorni solari dalla data di avvio del trasferimento che sarà indicata dall'Amministrazione;
- per tutta la durata del trasferimento il Fornitore continuerà ad erogare i servizi di propria pertinenza.

Il Piano di trasferimento (PTF) è un documento che dovrà prevedere almeno i seguenti contenuti minimi:

- l'oggetto del trasferimento;
- le attività e le relative modalità di esecuzione;
- i compiti e le responsabilità di ciascuna delle Parti;
- il programma temporale in base al quale le attività dovranno essere eseguite.

Il PTF dovrà essere redatto dal Fornitore ed aggiornato a seguito delle modifiche richieste dall'Amministrazione ovvero intervenute nel corso di svolgimento delle attività di trasferimento (ad esempio a seguito del riesame congiunto con il Fornitore Subentrante nella fase di subentro, o anche successivamente durante lo svolgimento delle attività di trasferimento per aggiunta/modifica o cancellazione di attività/riunioni).

La responsabilità della gestione contrattuale viene mantenuta dal Fornitore fino al termine delle attività di trasferimento del servizio specifico (o parte di esso) in conformità di quanto previsto dal PTF.

## **7.4 Exit Strategy e Grace Period**

Fermo restando quanto previsto al paragrafo 12.2 del Capitolato Tecnico Generale per le soluzioni cloud eventualmente offerte e per le infrastrutture, con riferimento a tutti i servizi trova applicazione quanto segue.

Al termine della durata contrattuale di ogni singolo Contratto esecutivo, per un periodo pari a 30 giorni, altrimenti detto grace period, il Fornitore si obbliga, senza oneri aggiuntivi, a mettere a

disposizione della PA i dati di quest'ultima, ai fini del relativo recupero. Il Fornitore si obbliga a dare idonee garanzie dell'eliminazione e/o avvenuta inaccessibilità dei dati della PA. In ogni caso, il Fornitore si impegna a dare supporto alla PA per il grace period, senza oneri aggiuntivi (Exit strategy).

Preliminarmente alla fase di Exit strategy, il Fornitore si obbliga a esportare i dati in un formato che andrà stabilito in accordo con la PA e, comunque, idoneo a consentire il trasferimento dei dati stessi e dei servizi.

Al termine di tale periodo di recupero, e a meno che non sia espressamente richiesto dalla legge, i dati della PA verranno cancellati e/o comunque resi inaccessibili. A tal fine, il Fornitore si obbliga a fornire tutte le idonee garanzie a dimostrazione della eliminazione dei dati nonché la disponibilità a far eseguire verifiche in tal proposito da parte della PA o di soggetti terzi da questa designati.

## 8 MODALITÀ DI EROGAZIONE

### 8.1 Risorse da impiegare nell'affidamento dei servizi

Il Fornitore garantisce che tutte le risorse che impiegherà per l'erogazione dei servizi oggetto della fornitura siano adeguate al ruolo ricoperto all'interno dei servizi e che, con particolare riferimento ai servizi di supporto specialistico, corrispondano almeno ai requisiti minimi espressi dal presente capitolato tecnico speciale e all'Appendice 2 "Profili Professionali", integrati con tutte le migliorie offerte in Offerta Tecnica.

Nel Piano dei fabbisogni, ove sia richiesto il servizio di supporto specialistico, è facoltà della singola Amministrazione specificare nel dettaglio le proprie esigenze indicando le figure professionali (ad esempio Information security consultant senior), il tipo di tariffa (ad esempio profilo base e/o profilo avanzato) e la quantità espressa in giorni persona e la modalità di remunerazione (a corpo/a consumo).

Per l'accettazione del personale proposto (tanto le risorse da impiegare nei servizi di supporto specialistico tanto i Responsabili tecnici ed eventuali ruoli aggiuntivi proposti), l'Amministrazione si riserva la possibilità di procedere ad un colloquio tecnico di approfondimento per verificare la corrispondenza delle competenze ed expertise riportate nel CV e l'effettivo possesso. In tal caso il Fornitore dovrà rendere disponibile al colloquio la risorsa entro 3 giorni lavorativi dalla richiesta.

Qualora l'Amministrazione ritenga inadeguato il suddetto personale essa procederà alla richiesta formale di sostituzione, anche nel periodo di Presa in carico e startup.

I vincoli temporali sotto riportati, unitamente a quanto previsto contrattualmente, devono essere considerati come scadenze contrattuali e dunque presidiati dagli indicatori di cui all'Appendice 1 Indicatori di Qualità.

Vincoli temporali			
Attività	Evento	Giorni	Note
Consegna all'Amministrazione dei CV delle risorse di supporto specialistico/eventuali ruoli aggiuntivi offerti per la fase di PRESA IN CARICO E STARTUP e dei responsabili tecnici	Stipula del contratto esecutivo	5 giorni lavorativi	Allegato al piano di PRESA IN CARICO E STARTUP

Vincoli temporali			
Attività	Evento	Giorni	Note
Consegna all'Amministrazione dei CV delle risorse professionali (di supporto specialistico/eventuali ruoli aggiuntivi offerti) e dei ruoli di interfaccia con l'Amministrazione	Stipula del Contratto esecutivo	10 giorni lavorativi	Allegato al piano di lavoro generale
Colloquio	Richiesta di colloquio	3 giorni lavorativi	
Disponibilità della risorsa professionale	Comunicazione dell'esito positivo del colloquio	3 giorni lavorativi	In funzione degli specifici piani approvati
Consegna dei CV all'Amministrazione a valle di una valutazione di non idoneità di una risorsa/sostituzione	Valutazione di non idoneità un CV/ Sostituzione risorsa	3 giorni lavorativi	
Disponibilità della risorsa in sostituzione	Comunicazione di valutazione positiva	3 giorni lavorativi	In funzione degli specifici piani approvati

Tabella 4 – Vincoli temporali

L'Amministrazione si riserva di chiedere la sostituzione del personale durante l'intera fornitura con la medesima modalità e tempi sopra riportati o maggior termine indicato dalla stessa Amministrazione.

## 8.2 Competenze richieste

Il Fornitore dovrà mettere in campo per l'erogazione dei servizi oggetto di fornitura tutte le competenze di natura tecnica, funzionale, metodologica e organizzativa, tali da affrontare le eventuali problematiche e proporre, realizzare e gestire le relative soluzioni, nei contesti specifici dell'Amministrazione.

Le competenze che il Fornitore mette a disposizione devono essere descritte, dimostrate, possedute e messe a disposizione a livello di Raggruppamento di Imprese o Consorzio, in termini di strutture organizzative, metodologie, centri di competenza, risorse professionali, esperienze pregresse. Nell'Appendice 2 al Capitolato Tecnico Speciale "Profili Professionali" sono indicate, per il servizio di supporto specialistico, le competenze, le conoscenze e le relative certificazioni/credenziali delle risorse professionali che dovranno essere impiegate dal Fornitore per l'esecuzione dei servizi.

### **8.3 Comunicazioni e Approvazioni**

I documenti richiesti contrattualmente devono essere notificati formalmente, in genere, sotto forma di verbale.

Il ciclo di vita dei documenti ufficiali dovrà essere definito nel Piano della Qualità Generale.

Si precisa che la mancata approvazione di documenti contrattuali (inclusi i deliverable dei servizi) costituisce inadempimento contrattuale cui può conseguire l'adozione delle azioni contrattuali indicate nell'Accordo Quadro e nell'Appendice 1 Indicatori di Qualità.

### **8.4 Modalità di Approvazione**

Tutte le comunicazioni inerenti all'approvazione (o mancata approvazione) dei prodotti della fornitura saranno notificati dall'Amministrazione al Fornitore. In nessun caso l'approvazione potrà avvenire per tacito assenso.

Il Fornitore dovrà aggiornare i prodotti soggetti a rilievi e/o mancata approvazione senza alcun onere aggiuntivo per la Amministrazione. Per tutti i prodotti della fornitura soggetti ad approvazione, la presenza di anomalie di gravità tale da impedire lo svolgimento delle attività di verifica comporta l'applicazione delle sanzioni contrattualmente previste.

I prodotti della fornitura che sono soggetti ad approvazione formale sono:

- Piano della Qualità Generale;
- Piano della Qualità specifico di Contratto esecutivo;
- Piano di presa in carico e startup;
- Piano di migrazione, ove previsto;
- Piani di lavoro di ciascun servizio;
- Piano di trasferimento di know-how (PTF);
- i deliverable obbligatori di ciascun servizio salva differente indicazione dell'Amministrazione nel Piano di qualità.

I restanti prodotti sono sottoposti a controllo (Accettazione/Verifica e Validazione) da parte dell'Amministrazione, che pertanto potrà non accettarli e richiedere di apportare le modifiche ritenute necessarie.

Per i servizi oggetto di fornitura, nel caso si verificano situazioni "anomale" che, a giudizio della Amministrazione, sia per numerosità, sia per gravità non consentano lo svolgimento o la prosecuzione delle attività, l'Amministrazione procederà alla sospensione delle verifiche di

conformità del servizio, la cui riattivazione dovrà avvenire entro il nuovo termine fissato dalla stessa Amministrazione.

## 8.5 Verifiche di conformità

L'Amministrazione è deputata all'esecuzione delle attività di verifica di conformità, dopo aver acquisito la documentazione tecnico-funzionale dei servizi (sia a canone che a corpo/a consumo), procederà a verificare la corretta esecuzione degli stessi.

## 8.6 Azioni contrattuali

Ogni inadempimento contrattuale darà origine ad un'azione commisurata alla criticità dell'inadempimento stesso. I principali aspetti delle prestazioni contrattuali vengono presidiati da appositi indicatori di qualità.

Il mancato rispetto dei requisiti minimi richiesti e/o migliorati dal fornitore in Offerta tecnica determina azioni contrattuali conseguenti che possono consistere in una o più delle seguenti azioni:

- coinvolgimento degli interlocutori istituzionali allo scopo di prendere le decisioni necessarie al ripristino delle situazioni fuori soglia o fuori controllo (attivazione di una procedura di escalation);
- ripetizione da parte del Fornitore dell'erogazione di una prestazione, rifacimento di una attività, riconsegna di un prodotto (chiusura di una non conformità);
- azione di intervento sui processi produttivi del fornitore per evitare il ripetersi di sistematiche non conformità (esecuzione di una azione correttiva);
- applicazione di rilievi e di penali;
- azioni aggiuntive (richiesta danni, risoluzione anticipata del contratto, ecc.) laddove previsto contrattualmente.

Segue un approfondimento degli istituti a tutela della qualità dell'erogazione della fornitura.

### Rilievi

I rilievi sono le azioni di avvertimento da parte della Amministrazione conseguenti il non rispetto delle indicazioni contenute nella documentazione contrattuale. Oltre a quanto esplicitamente previsto potrà essere emesso un rilievo su qualunque inadempimento se non diversamente sanzionato.

I rilievi non prevedono di per sé l'applicazione di penali, ma costituiscono avvertimento sugli aspetti critici della fornitura e, se reiterati e accumulati, danno luogo a penali, secondo quanto previsto in Appendice 1 Indicatori di Qualità.

I rilievi possono essere emessi dal Direttore dell'esecuzione della Amministrazione, dai responsabili di progetto e/o di servizio della Amministrazione e/o da strutture della Amministrazione preposte o di supporto al controllo e/o monitoraggio della fornitura e sono formalizzati attraverso una nota di rilievo, ognuna delle quali potrà contenere uno o più rilievi.

Qualora il fornitore ritenga di procedere alla richiesta di annullamento del rilievo, dovrà sottoporre all'Amministrazione un documento con elementi oggettivi ed opportune argomentazioni entro 3 giorni lavorativi dall'emissione del rilievo.

### **Penali**

Lo scopo delle penali è riequilibrare il servizio effettivamente ricevuto (di minore qualità, e/o generando disservizi e/o ritardi e/o inducendo un danno all'utilizzatore) dall'Amministrazione al corrispettivo da erogarsi che è stabilito per prestazioni effettuate nel rispetto dei requisiti e da Consip in relazione al mancato rispetto degli impegni dell'Accordo quadro.

Per il dettaglio del processo di contestazione ed applicazione delle penali, si rinvia a quanto disciplinato nel contratto.

## **8.7 Monitoraggio**

Le attività di monitoraggio dovranno essere conformi a quanto previsto dalla circolare n. 1 del 20 gennaio 2021 emessa dall'AgID, ai sensi dell'art. 14-bis, comma 2, lett. h.) del CAD, come modificato dal decreto legislativo 26 agosto 2016, n. 179.

La funzione di monitoraggio sarà svolta dall'Amministrazione o da soggetto da essa incaricato.

Il Fornitore si impegna a fornire all'Amministrazione tutti i documenti necessari all'attività di monitoraggio nei formati richiesti e necessari per il controllo e la verifica della fornitura, salvo evoluzioni derivanti dall'introduzione, da parte dell'Amministrazione, di strumenti automatici a ciò deputati.

Il Fornitore si impegna ad inviare all'Amministrazione la documentazione comprovante l'eventuale esito delle visite di sorveglianza della società di certificazione della qualità e/o il rinnovo della certificazione entro 1 mese dalla data della verifica.

Il Fornitore e/o i subfornitori devono rendersi disponibili alle verifiche anche ispettive effettuate dall'Amministrazione tramite personale proprio o da terzi da essa incaricati, svolte nel rispetto di quanto prescritto dalla serie di norme EN ISO 19011:2003.

### **Reportistica e strumenti di monitoraggio**

Ai fini del monitoraggio sull'andamento dei singoli Contratti esecutivi e dell'Accordo Quadro nel suo complesso si prevede che il Fornitore produca dei report alle singole Amministrazioni contraenti e, se richiesto a Consip.

Il Fornitore dovrà garantire adeguati livelli di riservatezza nel trattamento delle informazioni documentali, secondo la normativa vigente.

In fase di attivazione dei singoli servizi nell'ambito dei Contratti esecutivi delle Amministrazioni contraenti o al momento della eventuale richiesta da parte di Consip, verranno concordati puntualmente per ciascun report il livello di dettaglio e di aggregazione dei dati.

Il Fornitore deve produrre un report contrattuale dei livelli di servizio conseguiti con relativo calcolo delle penali e dei servizi erogati.

Tale report, prodotto in formato file .ods e .xls, dovrà essere fruibile mediante una piattaforma di monitoraggio messa a disposizione del Fornitore senza oneri aggiuntivi per l'Amministrazione (o inviato via PEC solo in caso di indisponibilità della piattaforma per malfunzionamento) coerente con la periodicità di fatturazione scelta dall'Amministrazione; pertanto, dovrà contenere i dati relativi agli oggetti di fornitura cui la fatturazione si riferisce, con l'opportuno livello di aggregazione.

La disponibilità del report dovrà essere comunicata via PEC alle Amministrazioni ai fini del monitoraggio dei livelli del servizio e dell'applicazione delle rispettive penali.

Il report dovrà essere fruibile dall'Amministrazione Contraente entro i **10 (dieci) giorni successivi** alla chiusura del periodo di riferimento, ai fini della verifica di conformità e rispettiva fatturazione.

## 8.8 Dimensionamento dei servizi

### A canone

Per i servizi con dimensionamento a canone, secondo quanto indicato al precedente capitolo 3 e relativi paragrafi, la responsabilità del risultato è affidata al Fornitore, il quale organizza le proprie risorse professionali, tecniche e metodologiche per soddisfare le richieste dell'Amministrazione. L'Amministrazione fornisce le macro esigenze partendo dal contesto funzionale e tecnologico.

Tali servizi vengono erogati senza soluzione di continuità, sulla base delle frequenze temporali stabilite nel presente capitolato per il servizio, nel rispetto degli orari previsti. Il Piano della qualità dovrà indicare nel dettaglio le modalità di erogazione, controllo e rendicontazione delle attività effettuate nell'ambito dei servizi continuativi.

I servizi con modalità a canone definiti sulla base di "classi incrementali" (es., classe 1: utenti fino a 250; classe 2: utenti fino a 500 ecc..) sono remunerati attraverso l'applicazione del prezzo unitario della fascia corrispondente alla quantità complessiva acquistata.

### A corpo

La modalità a corpo può essere utilizzata solo per i servizi di supporto specialistico, secondo quanto indicato al precedente paragrafo 3.13. Nella modalità a corpo la responsabilità del risultato è affidata al fornitore, il quale organizza le proprie risorse professionali, tecniche e metodologiche per soddisfare le richieste.

L'Amministrazione fornisce le macro esigenze partendo dal contesto funzionale e tecnologico.

Con l'approvazione del piano di lavoro, il fornitore ne è responsabile, e pertanto non potrà richiedere maggiori costi o tempi per le attività previste. Il fornitore risponderà dei danni causati da errata allocazione o non adeguatezza delle risorse, difettosità della soluzione, ecc., cui dovrà rimediare a proprie spese per rilasciare un prodotto conforme funzionalmente e tecnicamente ai requisiti approvati.

Il servizio erogato in modalità progettuale a corpo presuppone tipicamente un Piano di lavoro le cui milestone sono le seguenti:

Milestone	Attore	Descrizione
<b>Richiesta stima e Piano di lavoro</b>	Amministrazione	Richiesta al fornitore di procedere alla stima dei tempi e costi dell'obiettivo
<b>Stima (pre-dimensionamento)</b>	Fornitore	Comunicazione dei tempi e dei costi previsti per il progetto
<b>Attivazione</b>	Amministrazione	Avvio del fornitore sulle attività progettuali
<b>Consegna</b>	Fornitore	Rilascio degli artefatti previsti dal piano di lavoro, sia intermedi che finali
	Amministrazione	Riscontro degli artefatti consegnati in quantità e tipologia (ricevuta), senza valutazione di contenuto
<b>Approvazione e Verifica di conformità (intermedia)</b>	Amministrazione	Validazione dei prodotti intermedi, previa verifica di merito. Certificazione della corretta esecuzione del servizio relativamente ai prodotti oggetto di approvazione.
<b>Accettazione e Verifica di conformità (finale)</b>	Amministrazione	Verifica e validazione dei prodotti, previo collaudo. Certificazione della corretta esecuzione del servizio relativamente ai prodotti oggetto di accettazione.

*Tabella 5 - Milestone*

L'Amministrazione richiede la stima ed il Piano di lavoro del singolo progetto, fornendo la documentazione di supporto ed i macro-requisiti per poter avviare la raccolta dei requisiti.

La documentazione di supporto è in genere corredata da un insieme di informazioni utili alla comprensione dell'obiettivo, quali ad esempio:

- data prevista di inizio attività;
- data prevista di fine attività;
- data limite richiesta per il completamento delle attività di raccolta Requisiti, stima e predisposizione del Piano di lavoro;

- date vincolo (ad esempio richieste utente di date di esercizio, scadenze normative, scadenze amministrative);
- riferimenti a documentazione esistente (ad esempio studi di fattibilità, requisiti utente già espressi, Roadmap di migrazione e Assesment, Modelli To Be forniti dall'Amministrazione, ecc.).

Il Fornitore presenterà il documento di stima dei dimensionamenti, piano di lavoro, razionali del dimensionamento ed i fattori di affidabilità e variabilità.

Alla consegna dei deliverable di stima e di Piano di lavoro, corredati dai razionali per la determinazione dei tempi e dei costi, l'Amministrazione procede con le verifiche e validazione al fine autorizzare la prosecuzione delle attività.

Il fornitore è tenuto a produrre la stima iniziale entro e non oltre il termine stabilito dalla Amministrazione.

Resta inteso che il dimensionamento è riconosciuto al buon esito delle verifiche di conformità e, pertanto, solo se il servizio prestato soddisfa tutti i requisiti espressi dall'Amministrazione, nei modi e tempi da essa indicati e rispettando tutti i livelli di qualità, di servizio e di obiettivo richiesti.

### **A consumo**

La modalità a consumo può essere utilizzata solamente per il supporto specialistico, secondo quanto indicato al precedente paragrafo 3.13, e presuppone una responsabilità limitata alla fornitura di risorse con adeguata competenza tecnico-professionale ed alla risoluzione di task con ampiezza contenuta e dipendente anche da direttive puntuali impartite dall'Amministrazione. La responsabilità del fornitore è limitata alle attività di volta in volta affidate. In questo caso, il fornitore non può essere responsabile della soluzione totale, ma i fattori rilevanti sono l'adeguatezza ai profili professionali richiesti, la competenza tecnica e funzionale, il rispetto degli orari di lavoro e della produttività richiesta.

## **8.9 Pianificazione e Consuntivazione**

### **Piano della Qualità Generale dell'Accordo quadro**

Il Piano della Qualità Generale dell'Accordo quadro è descritto nel Capitolato Tecnico Generale.

Il Fornitore dovrà mantenere il proprio Piano di Qualità aggiornato allo stato della tecnologia, di automazione, misurazione e controllo e potrà specializzare e definire puntuali integrazioni o modifiche al Piano di Qualità Specifico del Contratto esecutivo.

Il RUAC è responsabile della piena applicazione ed aggiornamento del Piano di Qualità a qualunque livello: a partire dall'inizio della fornitura e con cadenza massima trimestrale dovrà riferire e consegnare a Consip i Rapporti sul rispetto del Piano di Qualità della fornitura ed i Rapporti di conformità su tutti gli impegni assunti in offerta tecnica.

### **Piano della Qualità Specifico di Contratto esecutivo**

Per ciascun Contratto esecutivo il fornitore dovrà produrre un Piano della Qualità personalizzato sulla configurazione ed erogazione degli specifici servizi oggetto di fornitura e sugli obiettivi dell'Amministrazione. Il piano è soggetto all'approvazione dell'Amministrazione.

Tale documento dovrà essere prodotto a partire dal Piano della Qualità Generale dell'Accordo Quadro e riportare le eventuali deroghe alle regole ereditate, la declinazione specifica per i servizi attivati nello specifico Contratto esecutivo.

Nella redazione del piano il Fornitore terrà come guida lo schema di riferimento di seguito descritto, evidenziando sia le caratteristiche qualitative relative a specifici servizi e sia le eventuali deroghe da quanto previsto nel Piano della Qualità Generale. Nel caso in cui per un determinato capitolo non ci siano differenze rispetto al Piano di Qualità Generale dell'AQ occorre solo riportare il riferimento al suddetto piano.

- Descrizione specifica del Contratto esecutivo;
- scopo del Piano della Qualità (elenca le motivazioni e le peculiarità dell'obiettivo dell'Amministrazione per le quali è richiesto il documento);
- documenti applicabili e di riferimento;
- ruoli e responsabilità di riferimento;
- modalità di erogazione, consuntivazione dei servizi;
- metodi, tecniche e strumenti specifici del servizio/attività (contiene l'indicazione dei metodi, delle tecniche, degli strumenti, degli standard di prodotto specifici del servizio solo se diversi da quelli descritti nel Piano della Qualità Generale dell'AQ);
- indicatori di qualità specifici del servizio (contiene gli attributi di qualità con riferimento alle metriche, ai valori limite-Valore di soglia- definiti negli indicatori di qualità);
- riesami, verifiche e validazioni (contiene l'elenco dei controlli da effettuare per il servizio e le modalità di esecuzione dei controlli comprensive sia degli strumenti da utilizzare e sia della modulistica di rendicontazione dei risultati, se diversi da quelli descritti nel Piano della Qualità Generale).

### **Piani di Lavoro**

Il Fornitore dovrà predisporre, con le tempistiche indicate nel Capitolato Tecnico Generale, e mantenere costantemente aggiornato il

Piano di lavoro generale che è comprensivo di:

- piano di Presa in carico e startup di inizio fornitura, pianificazione delle attività trasversali di carattere generale ad esempio: pianificazione delle attività di assicurazione della qualità;
- piano di lavoro dei servizi che si estrinsecherà in un piano per ogni servizio.

A fronte di ripianificazioni autorizzate dall'Amministrazione, il Fornitore redigerà e consegnerà la versione aggiornata del Piano di lavoro.

Il Fornitore è tenuto a comunicare - entro il giorno lavorativo successivo al verificarsi dell'evento - qualsiasi criticità, ritardo o impedimento che modificano il piano concordato e ad inviare una ripianificazione delle attività, aggiornando e riconsegnando il relativo Piano di Lavoro.

In nessun caso potrà essere rivisto il Piano di Lavoro in seguito ad uno o più rilievi emessi su deliverable che costituiscono milestone di fine attività; si precisa che la mancata approvazione di documenti contrattuali e/o artefatti di servizi costituisce inadempimento contrattuale.

In qualunque momento l'Amministrazione può richiedere la consegna del Piano di Lavoro. Questo dovrà contenere tutti gli aggiornamenti concordati. Il Piano di Lavoro e le sue modifiche certificano ai fini contrattuali gli obblighi formalmente assunti dal Fornitore, e accettati dall'Amministrazione, su misurazioni e tempi di esecuzione dei servizi.

### Stato Avanzamento Lavori

Il Fornitore dovrà mantenere aggiornata la sezione relativa allo stato di avanzamento dei lavori contenuta nei Piani di Lavoro approvati, fornendo sulla base della tempistica di aggiornamenti definita nel Piano di Qualità specifico del Contratto esecutivo e dalle necessità del singolo servizio, o su richiesta dell'Amministrazione, indicazioni sulle attività concluse ed in corso, esplicitandone la percentuale di avanzamento, su eventuali rischi/criticità/ritardi, su eventuali impatti dei rischi/criticità, su azioni di recupero e razionali dello scostamento.

Per le attività continuative la frequenza minima di aggiornamento è mensile, mentre per le attività progettuali a corpo/a consumo, la frequenza minima di aggiornamento è di 2 settimane, salvo diverso accordo con l'Amministrazione.

### Consuntivazione

La consuntivazione delle attività svolte dovrà essere predisposta dal Fornitore mensilmente nella sezione Stato Avanzamento Lavori di ciascun Piano di lavoro relativamente a ciascun servizio.

Il piano di lavoro dovrà essere corredato dal Rendiconto Risorse per i servizi che prevedono un dimensionamento progettuale a corpo/a consumo.

La consuntivazione delle attività svolte dovrà dare evidenza delle fasi chiuse e riportare gli eventuali scostamenti rispetto alla pianificazione concordata.

## 8.10 Orario di erogazione dei servizi

Di seguito gli orari di servizio della fornitura.

Ambito dei Servizi	Orario
Supporto Specialistico	Orario base: lunedì – sabato: 08:00 – 20:00 Orario avanzato: lunedì - sabato 20:00 – 8:00, domeniche e festivi

Servizi Managed Security Services (ivi compresa la disponibilità di Service Desk, gestione del processo di Incident Response)	H24, 7 gg su 7, 365 gg anno
---	-----------------------------

Tabella 6 - Orari di servizio

L'Amministrazione nel piano dei fabbisogni indicherà il proprio orario di servizio.

Per l'impiego di risorse professionali, si precisa che il sabato è compreso nei giorni feriali. Il sabato è evidenziato distintamente per fornire una rappresentazione media delle effettive richieste di erogazione dei servizi, ma si precisa che nessuna maggiorazione di prezzo è applicabile al sabato per l'orario 08:00 – 20:00.

Si precisa che:

- è ammessa una flessibilità di 30 minuti sull'orario di inizio/fine di erogazione;
- la copertura temporale potrà essere differenziata per servizio indicando le modalità nel piano di lavoro;
- per festività devono intendersi solamente le festività a carattere nazionale e le domeniche, salvo casi indicati dall'Amministrazione in cui non vi siano servizi attivi.
- la tariffa giornaliera offerta è riferita a 8 ore lavorative.

Con particolare riferimento al servizio di supporto specialistico, l'Amministrazione, nel Piano dei Fabbisogni dovrà indicare in dettaglio i giorni della settimana e le fasce orarie giornaliere previste di operatività del servizio e dovrà dimensionare opportunamente il numero e la tipologia delle risorse professionali richieste. Laddove l'orario di servizio previsto sia esteso oltre le 40 ore lavorative settimanali, l'Amministrazione, nel dimensionamento delle risorse, dovrà tenere conto delle necessarie turnazioni e/o di ingressi/uscite differenziati, al fine di garantire la copertura complessiva del servizio nel rispetto dei limiti orari di disponibilità sopra indicati per la singola risorsa.

Può essere necessario, in relazione a esigenze dell'Amministrazione, non sempre prevedibili con la pianificazione mensile, un prolungamento dell'orario, all'interno delle fasce di cui alla Tabella precedente, dei servizi o la disponibilità di servizio il sabato.

La procedura di dettaglio concordata sarà tracciata nei Piano della Qualità Generale e Specifico e nel Piano di lavoro generale vengono indicati le esigenze temporali e quantitative di prolungamento dell'orario.

Il preavviso minimo di prolungamento dell'orario di servizio è il seguente:

- nella stessa giornata lavorativa: 4 ore lavorative;
- disponibilità la domenica e/o nei giorni festivi: 8 ore lavorative.

L'Amministrazione potrà richiedere l'estensione dell'orario di servizio via posta elettronica. Il Fornitore dovrà accettare la richiesta se pervenuta nel periodo di preavviso prestabilito.

I volumi di attività da effettuarsi in orario avanzato saranno indicati dall'Amministrazione committente in fase di dimensionamento del servizio, a valle della stipula del Contratto esecutivo.

La rilevazione e misurazione degli indicatori di qualità dovranno tenere conto dell'orario avanzato.