CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296

LOTTO 1

ALLEGATO 2A - CAPITOLATO TECNICO SPECIALE SERVIZI DI SICUREZZA DA REMOTO

Indice

1 Premessa

Il presente capitolato è parte integrante della documentazione di gara e definisce le caratteristiche e i requisiti per l'affidamento dei servizi di Sicurezza 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 - Lotto 1

Appendice 2 – Profili Professionali - Lotto 1

2 Oggetto

Relativamente al **Lotto 1**, l'oggetto della fornitura comprende i seguenti servizi:

ID Servizio	Servizio
L*1*.S1	Security Operation Center
L*1*.S2	Next Generation Firewall
L*1*.S3	Web Application Firewall
L*1*.S4	Gestione continua delle vulnerabilità di sicurezza
L*1*.S5	Threat Intelligence & Vulnerability Data Feed
L*1*.S6	Protezione navigazione Internet e Posta elettronica
L*1*.S7	Protezione end point
L*1*.S8	Certificati SSL
L*1*.S9	Formazione e security awareness
L*1*.S10	Gestione dell'identità e l'accesso utente
L*1*.S11	Firma digitale remota
L*1*.S12	Sigillo elettronico
L*1*.S13	Timbro elettronico
L*1*.S14	Validazione temporale elettronica qualificata
L*1*.S15	Servizi specialistici

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

- L1; ove è l'identificativo del Lotto;
- S*n;* 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 oggetto di fornitura saranno erogati nelle seguenti modalità:

- da remoto;
- on-site.

I servizi di sicurezza da remoto dovranno essere erogati secondo un modello "managed services" ovvero gestiti dal Fornitore in logica di continuità operativa; pertanto il Fornitore, in coerenza con i requisiti del Capitolato, dovrà garantire:

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

A tal fine è di fondamentale importanza che il Fornitore si interfacci efficacemente con le strutture interne dell'Amministrazione, in modo da poter concretizzare le strategie di cyber security adottate in risultati operativi ed il raggiungimento di obiettivi complessivi.

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.

I servizi dovranno essere erogati mediante l'impiego di personale esperto, con elevato grado di specializzazione e con una profonda conoscenza del contesto della sicurezza informatica. Inoltre, le tecnologie adottate dal Concorrente che sottendono l'erogazione dei servizi oggetto di fornitura dovranno garantire una costante 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. 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, integrandoli con il Portale della Fornitura e garantendone l'accessibilità e l'aggiornamento continuo.

Il Fornitore dovrà svolgere i servizi oggetto di fornitura nel rispetto della normativa, della regolamentazione di settore, nonché delle linee guida AgID vigenti e delle eventuali successive modificazioni.

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

La modalità di esecuzione dei servizi di sicurezza oggetto del lotto 1 è **da remoto** mediante i Centri Servizi messi a disposizione del Fornitore, salvo per i servizi ove è diversamente specificato.

I servizi di sicurezza oggetto di fornitura possono essere raggruppati in modo omogeneo in base all'obiettivo a cui sono preposti come indicato nella seguente tabella:

OBIETTIVO	SERVIZIO
Prevenzione e gestione delle minacce	Security Operation Center
	Next Generation Firewall
	Web Application Firewall
	Protezione navigazione Internet e Posta elettronica
	Protezione degli end-point
	Gestione continua delle vulnerabilità di sicurezza
	Threat Intelligence & Vulnerability Data Feed
	Formazione e security awareness
	Certificati SSL
Autenticazione degli accessi e validità probatoria	Gestione dell'identità e l'accesso utente
	Firma digitale remota
	Sigillo elettronico
	Timbro elettronico
	Validazione temporale elettronica qualificata
Supporto al delivery e alla migrazione dei servizi	Servizi specialistici

3.1 Servizi per la prevenzione e gestione delle minacce

3.1.1 L1.S1 - Security Operation Center (SOC)

1.1.1.1 Requisiti tecnico-funzionali del servizio

Il servizio di "Security Operation Center" (SOC) è il centro da cui vengono forniti i servizi alle Amministrazioni servizi mirati a garantire la corretta operatività dei sistemi attraverso la prevenzione, gestione, risoluzione di qualsiasi criticità di sicurezza che possa degradare il servizio all'utenza. La sua finalità principale è di gestione e monitoraggio dei servizi di sicurezza oggetto di fornitura e, in aggiunta, ricevere ed analizzare ad esempio la reportistica e di log dando anche la giusta priorità ai processi di risoluzione e/o mitigazione delle minacce.

Il Fornitore, nell'ambito del servizio "Security Operation Center" dovrà garantire all'Amministrazione almeno la disponibilità delle seguenti funzionalità base / strumenti a supporto:

- la capacità di identificazione, gestione, mitigazione e risoluzione degli attacchi alla sicurezza di sistemi dell'Amministrazione;
- la centralizzazione di tutte le attività di gestione delle funzionalità di sicurezza legate al Sistema Informativo (rete, sistemi, dati ed applicazioni);
- il monitoraggio in tempo reale dell'infrastruttura IT e di Sicurezza al fine di individuare tempestivamente tentativi di intrusione, di attacco o di minaccia dei sistemi;
- la raccolta centralizzata e attraverso canali cifrati (SSL) dei log e degli eventi generati da applicazioni e sistemi in rete (Security information Event managent - SIEM), anche da sistemi di sicurezza di tipo "on-site" gestiti dell'Amministrazione (ad esempio Firewall);
- la disponibilità di un Console di gestione / Portale dei Servizi di Sicurezza per effettuare ad es. la gestione delle configurazioni di policy o per effettuare nuove richieste di servizi;
- interazione con la piattaforma di trouble ticket del Centro servizi per la gestione delle richieste e la definizione degli alert e report;
- la capacità di correlazione tra eventi diversi raccolti dal SIEM, integrando ed analizzando eventi provenienti da fonti diverse e consentendo, in aggiunta a regole predefinite, la creazione di regole personalizzate;
- la disponibilità di un cruscotto (dashboard) che fornisca agli analisti, in tempo reale, una rappresentazione della situazione dei sistemi di sicurezza categorizzando per tipo di dispositivo e di dato, e la presenza di eventi anomali;
- il supporto operativo e di analisi per la rilevazione di codici malevoli al fine di identificare, insieme all'eventuale supporto specialistico, le corrette politiche di difesa e prevenzione, concorrendo all'indagine per l'individuazione di comportamenti anomali e malevoli;
- la produzione di report periodici di sintesi, di incident-report di dettaglio ed istruzioni operative per consentire analisi degli incident, contromisure adottate e procedure operative.

1.1.1.2 Metrica e modalità di remunerazione

La metrica del servizio di "Security Operation Center" è:

- **Device equivalenti/anno**

Il numero di Device equivalenti si calcola come rapporto tra il numero di Eventi Per Secondo richiesti (EPS) e il coefficiente EPS/Device relativo alla fascia di appartenenza, come di seguito indicato:

FASCIA – EVENTI PER SECONDO (EPS)	COEFFICIENTE (EPS/DEVICE)
Fascia 1: Fino a 300 EPS	6
Fascia 2: Fino a 600 EPS	7
Fascia 3: Fino a 1.200 EPS	8
Fascia 4: Fino a 6.000 EPS	10
Fascia 5: > 6.000 EPS	12

Esempio di calcolo per 4.000 EPS:
4.000 EPS ricade nella Fascia 4.
Il coefficiente (EPS/Device) è pari a 10.
Il numero di Device Equivalenti è pari a: 4.000/10 = 400
Il Canone annuale verrà calcolato come prodotto tra 400 * per il prezzo unitario offerto per la fascia di riferimento.

La modalità di remunerazione del servizio di "Security Operation Center" è:

- **Canone annuale**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

3.1.2 L1.S2 - Next Generation Firewall

1.1.1.3 Requisiti tecnico-funzionali del servizio

Il servizio di Next Generation Firewall dovrà consentire alle Amministrazione di filtrare tutto il traffico che i dispositivi di rete scambiano sia internamente che esternamente rispetto a un determinato perimetro, 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 Fornitore, nell'ambito del servizio di Next Generation firewall, dovrà garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità:

- funzionalità standard firewall (es. policy enforcement, statefull inspection, packet filtering, NAT, VPN client-to-site e site-to-site);
- sistema integrato di rilevamento e prevenzione delle intrusioni (IDS, IPS) per il blocco delle minacce;
- controllo delle applicazioni con blocco dell'esecuzione in funzione della configurazione impostata dall'Amministratore;
- ispezione approfondita del traffico di rete con analisi delle intestazioni e del contenuto di ogni pacchetto che transita nel perimetro di riferimento;
- visibilità del traffico crittografato con protezione da relative minacce tramite analisi del traffico https e altro traffico TLS/ SSL crittografato;
- blocco delle minacce in tempo reale. Protezione in tutte le fasi di un attacco e prevenzione rispetto a vulnerabilità conosciute e virus (anti-malware, anti-spam e anti-botnet inspection);
- QoS band-with management 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;
- 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;
- 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.

1.1.1.4 Metrica e modalità di remunerazione

La metrica del servizio di "Next Generation Firewall" è:

- **Ngfw Throughput/anno**

secondo le seguenti fasce:

- Fascia 1: fino a 250 Mbps
- Fascia 2: fino a 2 Gbps
- Fascia 3: fino a 4 Gbps
- Fascia 4: fino a 7 Gbps
- Fascia 5: fino a 15 Gbps
- Fascia 6: > 15 Gbps

La modalità di remunerazione del servizio di "Next Generation Firewall" è:

- **Canone annuale**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

3.1.3 L1.S3 - Web Application Firewall

1.1.1.5 Requisiti tecnico-funzionali del servizio

Il servizio di "Web Application Firewall" dovrà fornire alle Amministrazioni di filtrare, monitorare e bloccare il traffico HTTP da e verso un servizio Web, 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 fornitore, nell'ambito del servizio di Web Application Firewall, dovrà garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità:

- protezione dagli attacchi più critici alle applicazioni web, quali ad esempio Iniezioni SQL, Cross-site scripting (XSS), inclusione di file e configurazioni di sistema impropri, dirottamento di sessioni, buffer overflow;
- capacità evoluta di filtraggio del traffico con possibilità di configurare l'utilizzo di whitelist e blacklist
- funzionalità di apprendimento automatico che consentano di individuare un modello di comportamento dell'utente per identificare il traffico benigno e dannoso delle applicazioni;
- rilevamento automatico della natura dei contenuti e rilevazione di attacchi che comportino la manomissione di cookie, sessioni o parametri;
- funzionalità di ispezione del traffico SSL criptato per tutti i tipi di minacce integrate;
- capacità di identificare/bloccare gli allegati XML che nascondono contenuti dannosi e di convalidare gli schemi per i messaggi SOAP. Protezione di Api e web services di qualsiasi natura;
- supporto per le regole di controllo degli accessi a livello di rete e componente basate sulla firma per rilevare le minacce note;
- 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;
- 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.

1.1.1.6 Metrica e modalità di remunerazione

La metrica del servizio di "Web Application Firewall" è:

- **Throughput http/anno**

secondo le seguenti fasce:

- Fascia 1: fino a 500 Mbps
- Fascia 2: fino a 5 Gbps
- Fascia 3: > 5 Gbps

La modalità di remunerazione del servizio di "Web Application Firewall" è:

- **Canone annuale**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

3.1.4 L1.S4 - Gestione continua delle vulnerabilità di sicurezza

1.1.1.7 Requisiti tecnico-funzionali del servizio

Il servizio di "Gestione continua delle vulnerabilità di sicurezza" dovrà consentire alle Amministrazioni, tramite un processo automatico di assesment delle vulnerabilità, di ottenere una fotografia precisa del livello e gravità del rischio a cui, in quel momento, sono esposti i propri sistemi informatici. Il servizio si avvarrà dell'utilizzo di uno scanner che produrrà un report con le specifiche indicazioni di rischio relative alle vulnerabilità rilevate.
Il servizio di "Gestione continua delle vulnerabilità di sicurezza" dovrà garantire almeno le seguenti funzionalità:

- capacità di scansione di tutti gli asset più rilevanti dell'Amministrazione quali ad esempio:
  - scansioni relative al networking e quindi ai dispositivi di rete;
  - scansioni relative agli host/server;
  - scansioni specifiche per le reti wireless;
  - scansioni relative alle Web application;
  - scansioni relative ai database.
- capacità di classificare i rischi individuando i livelli di gravità;
- utilizzo dei "Common Vulnerability Scoring System (CVSS)" (punteggio numerico per ogni vulnerabilità rilevata) e loro traduzione in una rappresentazione qualitativa (ad. Es. basso, medio, grande), consentendo quindi la prioritizzazione dei processi di gestione delle vulnerabilità;
- possibilità di creare policy pre-impostate per l'esecuzione delle scansioni con opzioni di configurazioni già predefinite;
- visualizzazione, anche grafica, dei risultati della scansione con elenco dei dispositivi individuati con eventuali descrizioni e vulnerabilità, elenco delle vulnerabilità con la loro classificazione e debolezze individuate sugli host scansionati;
- possibilità di generare un report PDF, in almeno due modalità:
  - Executive Summary: un unico foglio riassuntivo per che viene avvisato della presenza di vulnerabilità;
  - Custom: che contiene L'elenco completo delle vulnerabilità con descrizione tecnica e soluzione da adottare;

  entrambi i report saranno a disposizione del referente dell'Amministrazione;
- disponibilità di uno storico di tutte le scansioni effettuate e meccanismi di estrazione efficace.

1.1.1.8 Metrica e modalità di remunerazione

La metrica del servizio di "Gestione continua delle vulnerabilità di sicurezza" è:

- **Numero di IP/anno**

secondo le seguenti fasce:

- Fascia 1: fino a 50 IP
- Fascia 2: fino a 200 IP
- Fascia 3: > 200 IP

La modalità di remunerazione del servizio di "Gestione continua delle vulnerabilità di sicurezza" è:

- **Canone annuale**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

3.1.5 L1.S5 - Threat Intelligence & Vulnerability Data Feed

1.1.1.9 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 garantire almento le seguenti funzionalità:

- disponibilità di feed di indicatori gratuiti (ad es SANS e CERT), feed a pagamento, bollettini, raccolte di informazioni interne ed altre fonti informative (aperte e non);
- disponibilità di interfacce di integrazione (API) per l'automazione dei report, consentendo la raccolta immediata di importanti dettagli, 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;
- disponibilità di flussi di Indicatori di Compromissione (domini sospetti, elenchi di hash malware noti, Indirizzi IP associati ad attività dannose, codice condiviso su Pastebin);
- disponibilità di vulnerability feed estratti dal National Vulnerability Database (NVD) quali ad es. vulnerabilità JSON, RSS.

1.1.1.10 Metrica e modalità di remunerazione

La metrica del servizio di "Threat Intelligence e Vulnerability Data Feed" è:

- **Data-Feed/anno**

secondo le seguenti fasce:

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

La modalità di remunerazione del servizio di "Threat Intelligence e Vulnerability Data Feed" è:

- **Canone annuale**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

3.1.6 L1.S6 - Protezione navigazione Internet e Posta elettronica

1.1.1.11 Requisiti tecnico-funzionali del servizio

Il servizio di Protezione internet e Posta elettronica 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.

Nel caso della posta elettronica, il servizio consente alle Amministrazioni di proteggersi da contenuti dannosi presenti nelle e-mail impedendo loro di raggiungere il destinatario previsto.

Il servizio si compone delle seguenti funzionalità:

- analisi del traffico per bloccare malware, botnet, spyware e furto dei dati;
- identificazione dei comportamenti potenzialmente pericolosi o non aderenti alle politiche aziendali. Blocco dei siti potenzialmente malevoli, consentendo o negando l'accesso ad un elenco di URL classificati;
- ispezione del traffico internet per vietare l'accesso ad un sito sulla base di una valutazione "risk based scoring" calcolata mediante informazioni di threat intelligence;
- aggiornamento automatico delle liste di siti malevoli;
- produzione di report di sintesi (executive summary) e di dettaglio (technical report);
- gestione della navigazione tramite utilizzo di categorie di siti web e protocolli;
- possibilità di controllare la banda utilizzata da siti di tipo Social Network, restringendone l'utilizzo a favore delle applicazioni di business;
- analisi del contenuto di ogni mail al fine di bloccare virus and malware, garantendo il costante aggiornamento dei "Threat pattern";
- filtraggio dello spamming ("spam filltering") con tecnologie di prefiltering che bloccano o mettono in quarantena le e-mail ricevute da "spammers" conosciuti, rilevano "patterns" già utilizzati in altre mail di spam e identificano link che puntano a siti/allegati malevoli;
- 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;
- filtraggio di documenti sensibili inviati per e-mail ad una casella esterna e/o blocco di file/immagini che contengono specifiche "keyword".

1.1.1.12 Metrica e modalità di remunerazione

La metrica del servizio di "Protezione internet e Posta elettronica" è:

- **Numero utenti/anno**

secondo le seguenti fasce:

- Fascia 1 - Fino a 1000 utenti
- Fascia 2 - Fino a 5.000 utenti
- Fascia 3 - Fino a 10.000 utenti
- Fascia 4 - Fino a 20.000 utenti
- Fascia 5 - > 20.000 utenti

La modalità di remunerazione del servizio di "Protezione internet e Posta elettronica" è:

- **Canone annuale**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

3.1.7 L1.S7 - Protezione degli end-point

1.1.1.13 Requisiti tecnico-funzionali del servizio

Il servizio di Protezione endpoint 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 conformi ai requisiti di conformità dell'Amministrazione.

Il fornitore, nell'ambito del servizio di Protezione endpoint, dovrà garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità:

- protezione dei dispositivi mediante sistemi antimalware (antivirus, antispam), impedendo lo sfruttamento delle carenze di sicurezza e l'accesso non autorizzato;
- Ispezione efficace 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;
- conformità agli standard 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 o l'esecuzione di un software antivirus aggiornato;
- monitoraggio continuo delle minacce avanzate e protezione da malware basati su file e senza file, supportando l'identificazione degli attacchi in fase iniziale e la risposta rapida ad un'ampia gamma di minacce (Endpoint Detection and Response – EDR);
- controllo dell'uso dei dispositivi USB e di altri device portatili prevedendo l'utilizzo non autorizzato di periferiche di archiviazione (ad es. pendrive, hard-disk esterni) ed attivando il controllo ed il monitoraggio di tutte le porte di comunicazione (ad es. USB, SATA, WI-FI);
- prevenzione della perdita di dati tramite USB, email, applicazioni SaaS, Web, dispositivi mobili e archiviazione nel cloud;
- crittografia dei file basata sulle policy aziendali per la protezione dei dati sensibili;
- 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.

1.1.1.14 Metrica e modalità di remunerazione

La metrica del servizio di "Protezione endpoint" è:

- **Numero nodi/anno**

  Secondo le seguenti fasce:

  - Fascia 1 - Fino a 500 nodi
  - Fascia 2 - Fino a 1.000 nodi
  - Fascia 3 - Fino a 5.000 nodi
  - Fascia 4 - > 5.000 nodi

La modalità di remunerazione del servizio di "Protezione endpoint" è:

- **Canone annuale**

L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

3.1.8 L1.S8 - Certificati SSL

1.1.1.15 **Requisiti tecnico-funzionali del servizio**

Il certificato SSL (Secure Sockets Layer) e il suo successore TLS (Transport Layer Security), sono protocolli standard necessari a garantire affidabilità e sicurezza della comunicazione tra le componenti client e server di un'applicazione internet. Il certificato assicura che le informazioni sensibili fornite dagli utenti sul web rimangano riservate e non vengano in alcun modo intercettate da terze parti (comunicazione criptata tra il client server e il server web).

Il Fornitore, nell'ambito del servizio di rilascio dei certificati SSL, dovrà garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità:

- utilizzo di certificati digitali sia lato server che, se richiesto, lato client;
- emissione da una Certification Authority (CA) accreditata al CA/Browser Forum (CAB Forum) e quindi ritenuto valido e riconosciuto world-wide dai principali browser e sistemi operativi;
- disponibilità alle Amministrazioni di tutte le tipologie di certificati SSL Server che, differenziandosi per le procedure di identificazione previste, consentano di soddisfare tutte le esigenze;
- possibilità per le Amministrazioni di richiedere certificati per la firma del codice, detti CodeSigning.

1.1.1.16 **Metrica e modalità di remunerazione**

La metrica del servizio di "Certificati SSL" è:

- **Numero certificati/anno**

secondo le seguenti fasce:

- fascia 1 SSL OV
- fascia 2 SSL OV Wildcard
- fascia 3 SSL EV
- fascia 4 SSL DV
- fascia 5 SSL Code Signing
- fascia 6 SSL Client Auth

La modalità di remunerazione del servizio di "Certificati SSL" è:

- **Canone annuale**

3.1.9 L1.S9 - Servizio di Formazione e Security awareness

1.1.1.17 Requisiti tecnico-funzionali del servizio

Il servizio "Formazione e Security awareness" è mirato a sensibilizzare l'Amministrazione su svariati aspetti della sicurezza delle informazioni, incrementando il livello di consapevolezza dei dipendenti, innalzando il livello di sicurezza dell'organizzazione e l'efficacia in termini di protezione dei dati aziendali critici e dei dati personali. Lo scopo è quello di sviluppare negli utenti le competenze essenziali, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e reagire al meglio a fronte di eventuali problemi.

Il servizio è erogato mediante la messa a disposizione di figure professionali da parte del Fornitore.

Si riportano a titolo esemplificativo e non esaustivo alcune tematiche che possono essere oggetto di formazione specifica:

- linee guida di base, ovvero la protezione del proprio computer e dei dispositivi mobili (smartphone e tablet);
- la robustezza e la protezione delle credenziali d'accesso;
- la salvaguardia delle proprie informazioni personali;
- il riconoscimento dei tentativi di intrusione e truffa (spam, phishing, social engineering, ecc.);
- governo delle politiche di sicurezza;
- analisi del rischio, anche in relazione agli strumenti e relative metodologie rese disponibili da Agid per la PA;
- le soluzioni di controllo e le migliori pratiche di prevenzione/risposta ad eventi negativi .

Devono essere disponibili pratiche formative tradizionali ed innovative, diversificate in funzione dell'area di appartenenza e della posizione aziendale, e con un forte taglio pratico ed adeguato rispetto alla platea dei fruitori.

A titolo indicativo, vengono riportate, in aggiunta alle modalità tradizionali di formazione in aula e e-learning, alcune tecniche formative innovative che dovrebbero essere utilizzate nella costruzione dei contenuti:

- allestimento di newsletter aziendali focalizzate di volta in volta su diverse tematiche di sicurezza delle informazioni, anche in funzione di eventi accaduti
- preparazione dei contenuti necessari ad alimentare il portale intranet aziendale in una sezione dedicata alla sicurezza
- preparazione di contenuti in modalità multimediale, specifici su alcune tematiche
- preparazione di apposite immagini di sensibilizzazione tali da consentirne la distribuzione sui diversi endpoint dei dipendenti

Dovranno essere utilizzate tecniche di verifica dei livelli di apprendimento raggiunti dai fruitori dei corsi in tema di cyber security. In aggiunta alle modalità più tradizionali di misura (es. test di verifica o interviste a campione per verificare i contenuti assimilati), dovranno essere individuate tecniche innovative, sensibilizzando i fruitori dei corsi tramite verifiche "sul campo", ad es. misurando l'efficacia delle credenziali da loro fornite oppure simulando un tentativo di "phishing" mostrando il risultato in termini di accesso ai dati personali.

1.1.1.18 Team di lavoro

Per erogare il presente servizio il fornitore dovrà disporre delle competenze, esperienze e capacità richieste a i profili professionali indicati nel seguito, che devono, tutte, **obbligatoriamente** fare parte del Team di Lavoro (o Team Ottimale) del servizio.

Il Team di Lavoro è sotto la responsabilità e l'organizzazione del fornitore.

Profili Professionali previsti nel Team di Servizio Formazione e Security awareness (per il dettaglio dei profili si rimanda all'appendice Profili Professionali)

- Security Principal
- Senior Information Security Consultant

- Junior Information Security Consultant

La tariffa offerta per il servizio in giorni persona si riferisce al Giorno Team Ottimale (pari a 8 ore lavorative).

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

1.1.1.19 Metrica e modalità di remunerazione

La metrica del servizio "Formazione e Security awareness" è:

- **Giorni/Persona del Team ottimale**

La modalità di remunerazione del servizio di "Formazione e Security awareness" è:

- **Progettuale (a corpo)**

La modalità di erogazione del servizio "Formazione e Security awareness" è scelta dall'Amministrazione e può essere:

- **on-site**
- **da remoto**

3.2 Autenticazione degli accessi e validità probatoria

3.2.1 L1.S10 - Gestione dell'identità e l'accesso utente

1.1.1.20 **Requisiti tecnico-funzionali del servizio**

Il servizio di Gestione dell'identità e dell'accesso utente (Identity & Access Management) dovrà consentire all'Amministrazione la completa gestione delle attività di identificazione, autenticazione ed autorizzazione propedeutiche all'accesso da parte di utenti esterni al portale dell'Amministrazione o ai servizi da essa erogati in rete. Per l'autenticazione dei propri utenti il servizio può fare ricorso ad un Identity provider esterno all'Amministrazione.

Il fornitore, nell'ambito del servizio di di Gestione dell'identità e dell'accesso utente, dovrà garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità:

- Gestione dei profili (creazione/migrazione); le Pubbliche Amministrazioni potranno aderire alle regole tecniche definite da SPID (specifiche SAML) senza dover realizzare e/o modificare le proprie infrastrutture tecnologiche;
- supporto della politica di "Policy Enforcement", per interfacciarsi con Identity Provider e Attribute Authority al fine di ricevere le richieste per l'applicazione delle policy di sicurezza associate alle risorse;
- supporto della politica di "Policy Decision" in grado di accedere ai i profili degli utenti e alle policy di sicurezza associate alle risorse per la verifica della legittimità della richiesta;
- gestione delle policy di accesso ai servizi e la gestione del ciclo di vita dei profili utente. Dovrà essere prevista la suddivisione degli utenti in gruppi omogenei tipo Role-based Access Control (RBAC);
- per la verifica degli attributi associati al profilo di un utente, esterni all'Amministrazione, il servizio farà ricorso ad Attribute Authority esterne;
- il gestore del servizio prevede, su richiesta, la presa in carico e la migrazione dei profili utente gestite dall'amministrazione;
- l'Amministratore dovrà poter accedere a una interfaccia web con visibilità dei soli dati degli utenti profilati per applicazioni erogate dalla propria Amministrazione e per le quali è referente a livello di Contratto es ecutivo;
- il gestore del servizio prevede, su richiesta, la presa in carico e la migrazione dei profili utente gestiti dall'Amministrazione.

Devono essere inoltre disponibili le seguenti funzionalità:

- ricerca di utente accreditato all'Amministrazione, visualizzazione dei suoi attributi identificativi e non, qualificati e profili applicativi correntemente assegnati;
- modifica dell'assegnazione dei profili applicativi;
- profilatura nuovo utente.

1.1.1.21 **Metrica e modalità di remunerazione**

La metrica del servizio di "Gestione dell'identità utente e l'accesso utente" è:

- **Numero di utenti/anno**

secondo le seguenti fasce:

- Fascia 1: fino a 10.000 utenti
- Fascia 2: fino a 100.000 utenti
- Fascia 3: fino a 500.000 utenti
- Fascia 4: > 500.000 utenti

La modalità di remunerazione del servizio di "Gestione dell'identità utente e l'accesso utente" è:

- **Canone annuale**

L’ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

3.2.2 L1.S11 - Firma digitale remota

1.1.1.22 **Requisiti tecnico-funzionali del servizio**

Il servizio di "Firma digitale" è un tipo di firma elettronica qualificata che dovrà consentire alle Amministrazioni di dare efficacia probatoria ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali. La firma digitale è il risultato di una procedura informatica, detta validazione, che garantisce l'autenticità, l'integrità e il non ripudio dei documenti informatici.

Il servizio dovrà prevedere quale modalità di utilizzo "da remoto": si intende la firma digitale generata usando strumenti di autenticazione (tipicamente user id+ password +OTP o telefono cellulare) che consentono la generazione della firma su un dispositivo (HSM) custodito dal prestatore del servizio fiduciario qualificato.

Beneficiari del servizio sono tutte le persone fisiche dipendenti di società e pubbliche amministrazioni di cui al capitolo 5 del Capitolato Tecnico Generale.
Il servizio dovrà essere configurato come un servizio online nel quale la chiave privata del firmatario viene generata e conservata assieme al certificato di firma rilasciato da parte di un Certificatore accreditato, all'interno di un server remoto sicuro (basato su un HSM conforme alla normativa vigente in materia).
E' quindi richiesto che venga utilizzato un sistema di autenticazione forte che preveda l'uso, oltre alla conoscenza di un codice segreto (es. PIN), di sistemi OTP fisici o logici (USB, telefono cellulare, token), eliminando in tal modo i problemi e i rischi relativi all'utilizzo delle sole password statiche.

Qualora il sistema di autenticazione preveda la fornitura di uno strumento fisico (es. OTP) ai titolari, la consegna è effettuata presso una sede dell'Amministrazione dalla stessa indicata. L'Amministrazione provvede alla consegna ai rispettivi titolari.
L'attività di verifica dell'identità dei titolari dei certificati di firma digitali, propedeutica al loro rilascio, è effettuata a cura e sotto la responsabilità dell'Amministrazione.

Il servizio dovrà essere reso in modo da garantire la conformità alla normativa vigente in materia di firme digitali (CAD d.lgs. 82 del 7 marzo 2005 e successive modifiche) e la Determinazione Commissariale n. 63/2014 dell'Agenzia per l'Italia Digitale.
Il servizio dovrà includere la fornitura dei certificati digitali rilasciati da un Ente Certificatore accreditato a norma e delle relative coppie di chiavi pubblica/privata con lunghezza minima di 2048 bit, necessarie alla generazione delle firme.

Il Fornitore, nell'ambito del servizio di Firma digitale remota dovrà garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità e/o strumenti a supporto:

- firma digitale remota dei documenti in formato CAdES, PAdES e XAdES come previsto dalla normativa vigente in materia;
- inserimento di firme multiple nello stesso documento;
- verifica delle firme digitali apposte a documenti informatici;
- gestione delle credenziali immateriali del sistema di autenticazione. Tali credenziali sono fornite ai titolari direttamente dall'Amministrazione;
- associazione degli strumenti fisici previsti dal sistema di autenticazione al singolo titolare;
- generazione e gestione delle richieste di emissione dei certificati di firma digitale;
- sottomissione e gestione delle richieste di revoca e sospensione dei certificati di firma digitale;
- firma digitale automatica massiva.

Dal punto di vista tecnico, il servizio dovrà prevedere almeno:

- alta disponibilità;
- messa a disposizione di un'interfaccia grafica;
- possibilità di integrazione con applicazioni tramite Web Services;
- funzionalità di verifica della firma compatibile con i principali formati di documenti (tra cui almeno .doc, .docx, .xls, .xslx, .pdf, .ppt, .pptx, .eml, .odt, .ods, .odp).
- La procedura di firma remota dovrà prevedere l'uso di un sistema di autenticazione a doppio fattore: conoscenza e possesso.

1.1.1.23 Metrica e modalità di remunerazione

La metrica del servizio di "Firma digitale remota" è:

- **Numero di utenti/anno (best effort)**

secondo le seguenti fasce:

- Fascia 1: > 50 e fino a 200 utenti
- Fascia 2: > 200 e fino a 500 utenti
- Fascia 3: > 500 e fino a 1.000 utenti
- Fascia 4: > 1.000 utenti

- **Numero di firme/sec (sla garantito).**

La modalità di remunerazione del servizio "Firma digitale remota" è:

- **Canone annuale**

3.2.3 L1.S12 - Sigillo elettronico

1.1.1.24 **Requisiti tecnico-funzionali del servizio**

Il servizio "Sigillo elettronico", al pari del servizio di "Firma digitale" di cui al precedente paragrafo 3.2.2 dovrà consentire alle Amministrazioni di dare efficacia probatoria ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali.

Beneficiari del servizio sono tutte le persone giuridiche, ovvero società e pubbliche amministrazioni di cui al capitolo 5 del Capitolato Tecnico Generale.
Relativamente ai requisiti minimi si fa riferimento a quanto indicato per il servizio di "Firma digitale remota" di cui al paragrafo 1.1.1.22.

1.1.1.25 **Metrica e modalità di remunerazione**

La metrica del servizio di "Sigillo elettronico" è:

- **Numero di Sigilli/secondo (sla garantito).**

La modalità di remunerazione del servizio "Sigillo elettronico" è:

- **Canone annuale**

3.2.4 L1.S13 - Timbro elettronico

1.1.1.26 **Requisiti tecnico-funzionali del servizio**

Il servizio di "Timbro elettronico" dovrà consentire alle Amministrazioni la creazione di documenti informatici che possano conservare la medesima validità legale anche dopo essere stati stampati su supporto cartaceo.
Il timbro digitale può essere indicato, anche in relazione alle specificità dello scenario, con termini differenti, quali "Contrassegno elettronico", "Codice bidimensionale", "Glifo".

In particolare, il servizio in oggetto dovrà consentire la creazione di un codice grafico bidimensionale posizionato in un punto qualsiasi del documento, a scelta dell'utente, e generato a partire dal contenuto del documento e dalla firma digitale, ove presente. Nell'ambito di tale servizio si richiede inoltre la messa a disposizione degli strumenti necessari per la decodifica del timbro e la verifica di conformità rispetto al documento originale.
Il servizio dovrà essere reso in modo da garantire la conformità alla normativa vigente in materia di timbro elettronico.

Il Fornitore, nell'ambito del servizio "timbro elettronico" dovrà garantire all'Amministrazione almeno la disponibilità delle seguenti funzionalità base / strumenti a supporto:

- creazione ed emissione del timbro elettronico;
- verifica del timbro elettronico e della conformità del documento stampato rispetto all'originale informatico; questa funzionalità dovrà poter essere liberamente e pubblicamente resa disponibile all'Amministrazione per la verifica dei documenti prodotti;
- gestione delle credenziali e creazione di specifici profili deputati all'apposizione del timbro.

Dal punto di vista tecnico, il servizio dovrà prevedere almeno:

- alta disponibilità;
- funzionalità di verifica del timbro compatibile con i principali formati di documenti (tra cui almeno .doc, .docx, .xls, .xslx, .pdf, .ppt, .pptx, .eml, .odt, .ods, .odp).

1.1.1.27 **Metrica e modalità di remunerazione**

La metrica del servizio di "Timbro elettronico" è:

- **Numero di timbrature**

secondo le seguenti fasce:

- Fascia 1: fino a 1.000 timbrature
- Fascia 2: > fino a 10.000 timbrature
- Fascia 3: > fino a 100.000 timbrature
- Fascia 4: > fino a 1.000.000 timbrature
- Fascia 5: > fino a 10.000.000 timbrature
- Fascia 6: > 10.000.000 timbrature

La modalità di remunerazione del servizio di "Timbro elettronico" è:

- **A consumo**

3.2.5 L1.S14 - Validazione temporale elettronica qualificata

1.1.1.28 **Requisiti tecnico-funzionali del servizio**

Il servizio di "Validazione temporale elettronica qualificata" (in precedenza qualificato come ""Marca temporale") dovrà fornire alle Amministrazioni, mediante un Certificatore accreditato, di associare data e ora, certe e legalmente valide, a un documento informatico, permettendo una validazione temporale del documento opponibile a terzi.
Il servizio permette quindi di garantire l'apposizione di un riferimento temporale certo (legalmente valido) sia a documenti firmati digitalmente sia a documenti non firmati, oltre che l'estensione della validità legale dei propri documenti firmati digitalmente nel tempo.
In definitiva permette di:

- dimostrare che lo specifico documento elettronico esisteva in quella firma alla specifica data;
- estendere la validità di un documento informatico, firmato digitalmente, oltre la data di scadenza del certificato di firma digitale.

Il servizio dovrà essere coerente con la definizione EIDAS che soddisfa i requisiti di cui all'articolo 42 del Regolamento eIDAS.

1.1.1.29 **Metrica e modalità di remunerazione**

La metrica del servizio di "Validazione temporale elettronica qualificata" è:

- **Numero di marcature (best effort)**

secondo le seguenti fasce:

- Fascia 1: fino a 1.000 marcature
- Fascia 2: fino a 10.000 marcature
- Fascia 3: fino a 100.000 marcature
- Fascia 4: fino a 1.000.000 marcature
- Fascia 5: fino a 10.000.000 timbrature
- Fascia 6: > 10.000.000 marcature

La modalità di remunerazione del servizio di "Validazione temporale elettronica qualificata" è:

- **Consumo**

- **Numero di marcature/sec. (sla garantito)**

La modalità di remunerazione del servizio di "Validazione temporale elettronica qualificata" è:

- **Canone annuale**

3.3 Supporto al delivery e alla migrazione dei servizi

3.3.1 L1.S15 - Servizi specialistici

1.1.1.30 **Requisiti tecnico-funzionali del servizio**

Il servizio "Servizi specialistici" dovrà fornire all'Amministrazione un supporto tecnico connesso all'attivazione dei servizi da remoto oggetto di fornitura.

Il servizio è erogato mediante la messa a disposizione di figure professionali da parte del Fornitore.

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

- supporto alla migrazione dei servizi di sicurezza dell'Amministrazione di tipo "on premise" verso i servizi oggetto di fornitura, nelle fasi di analisi e configurazione;
- attività di delivery dei servizi oggetto di fornitura durante le operazioni di migrazione;
- supporto nella definizione, configurazione ed erogazione del servizio di monitoraggio continuo delle vulnerabilità di sicurezza con particolare riferimento all'analisi dei deliverable raccolti a seguito dell'esecuzione da parte del fornitore delle sessioni di vulnerability assessment previsto nel servizio di cui al paragrafo 3.1.4.

1.1.1.31 **Team di lavoro**

Per erogare il presente servizio il fornitore dovrà disporre delle competenze, esperienze e capacità richieste ai profili professionali indicati nel seguito, che devono, tutte, **obbligatoriamente** fare parte del Team di Lavoro (o Team Ottimale) del servizio.

Il Team di Lavoro è sotto la responsabilità e l'organizzazione del fornitore.

Profili Professionali previsti nel Team di Servizio Servizi Specialistici (per il dettaglio dei profili si rimanda all'appendice Profili Professionali)

- Security Principal
- Security Solution Architect
- Senior Information Security Consultant
- Junior Information Security Consultant

La tariffa offerta per il servizio in giorni persona si riferisce al Giorno Team Ottimale (pari a 8 ore lavorative).

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

1.1.1.32 **Metrica e modalità di remunerazione**

La metrica del servizio "Servizi specialistici" è:

- **Giorni/Persona del team ottimale**

La modalità di remunerazione del servizio di "Servizi specialistici" è:

- **Progettuale (a corpo)**

La modalità di erogazione del servizio "Servizi specialistici" è scelta dall'Amministrazione e può essere:

- **on-site**
- **da remoto**

4 CENTRI SERVIZI

L'erogazione dei servizi in modalità *"da remoto"*, indicati nel presente Capitolato, richiede che il Fornitore dovrà disporre obbligatoriamente di Centri Servizi.
I Centri Servizi dovranno essere obbligatoriamente dislocati su sedi ubicate sul territorio comunitario. È fatto obbligo inoltre 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 e nel rispetto della normativa.
Il Centro Servizi – inteso come la struttura complessiva all'interno della quale è ritagliata dal Fornitore l'infrastruttura dedicata alle Amministrazioni contraenti - ed il personale ad esso addetto potranno non essere esclusivamente dedicati alla erogazione dei servizi di cui al presente Capitolato ma dovranno, comunque, rispettare i requisiti di cui al presente capitolato
Il Fornitore dovrà indicare in Offerta tecnica l'ubicazione dei Centri Servizi e le relative 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 remoti il Fornitore dovrà darne comunicazione formale ad AGID/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. L'interconnessione alla rete Internet dovrà avvenire per il tramite di almeno due differenti Service Provider afferenti a due POP con cammini distinti.
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 attuativi.
Tutte 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.
L'interconnessione alla rete SPC dovrà avvenire per il tramite di uno dei Fornitori qualificati SPC ai sensi del DLgs 42/2005.
Per le singole Amministrazioni non è previsto alcun onere aggiuntivo per la predisposizione e l'utilizzo della connessione telematica nell'ambito di ogni servizio.
Il Fornitore dovrà disporre di un proprio Autonomus System (AS) e di classi di indirizzi IP ad esso associate. Tali classi dovranno essere annunciate in maniera più specifica verso la rete SPC rispetto alle modalità di annuncio utilizzate verso la rete Internet.
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 adeguati sistemi e metodologie, nel rispetto di quanto stabilito dallo standard ISO/IEC 27001, oltre che gestite in piena conformità con la normativa vigente.

Devono essere soddisfatti dal Fornitore, almeno nei punti di contatto tra la rete dei Centri Servizi e la rete SPC, nell'ambito della presente gara, i livelli minimi di sicurezza previsti del sistema SPC, ovvero da quanto stabilito dal DPCM 1 Aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale»." G.U. 21 giugno 2008, n. 144.

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

- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI),** 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
Procedura di Gestione dei documenti SGSI	§3.1.1	Prima consegna alla stipula dell'Accordo Quadro; successivi aggiornamenti entro 30gg lavorativi dalla richiesta
Piano di Sicurezza del Centro Servizi	§3.1.2	Prima consegna alla stipula dell'Accordo Quadro; successivi aggiornamenti entro 30 gg lavorativi dalla richiesta

Consip/AgID si riservano la possibilità di eseguire un collaudo dei Centri Servizi secondo le modalità esplicitate nel paragrafo 7.3 del Capitolato Tecnico Generale.

4.1.1 Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

Il Fornitore dovrà prevedere per il Centro Servizi l'instaurazione di un adeguato sistema di gestione della sicurezza delle informazioni (SGSI), consistente in un processo iterativo articolato in successive implementazioni, monitoraggi e successive fasi di riesame e miglioramento.
Il perimetro di validità del SGSI 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 contrattuali.
Il Fornitore dovrà implementare il proprio SGSI 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 4.6 del Capitolato tecnico generale.
Consip/AgID si riservano la facoltà di richiedere durante la durata del contratto la documentazione di attuazione del SGSI prodotta dal Fornitore, il quale dovrà consegnarla entro 30 giorni dalla richiesta; tale documentazione dovrà essere mantenuta costantemente aggiornata in relazione alle successive evoluzioni del sistema.
La documentazione inerente l'SGSI dovrà essere gestita in modo da assicurarne il livello di protezione adeguato. 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;
- assicurarsi che la distribuzione dei documenti sia controllata.

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 del SGSI il Fornitore dovrà rendere disponibili su richiesta di Consip/AgID i seguenti deliverable:

Deliverable	Descrizione	Data di disponibilità
Documento di gestione delle registrazioni	Definire e manutenere le registrazioni che forniscono evidenza della conformità ai requisiti e dell'efficace operatività del SGSI (es.: libro dei visitatori, le registrazioni degli audit e l'autorizzazione per gli accessi fisici e logici, ecc.)	Documento entro 30 giorni lavorativi dalla richiesta
Programma e procedura Audit	Predisposizione procedura e conduzione di audit interni sul proprio SGSI ad intervalli pianificati, con cadenza almeno annuale, al fine di determinare se gli obiettivi del controllo, i controlli, i processi e le procedure del SGSI	Procedura entro 30gg lavorativi dalla stipula del Accordo Quadro e ad 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/AgID, 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 la reiterazione coerentemente con la procedura documentata di audit, da presentare a Consip/AgID su richiesta.	Template entro 30gg lavorativi dalla stipula del Accordo Quadro e ad ogni successivo aggiornamento
Processo di Incident Management e criteri di classificazione degli incidenti di sicurezza	Predisporre la documentazione descrittiva del processo di Incident Management, contenente i criteri di classificazione degli incidenti di sicurezza da presentare a Consip/AgID su richiesta.	Entro 30gg lavorativi dalla stipula del Accordo Quadro e ad ogni successivo aggiornamento
Template per il Riesame del SGSI	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 SGSI. I risultati del riesame sono documentati all'interno di un'apposita Relazione di riesame del Fornitore. Consip/Agid si riservano di effettuare controlli in un qualsiasi momento.	Entro 30gg lavorativi dalla stipula del Accordo Quadro e ad ogni successivo aggiornamento
Valutazione dei rischi	Predisporre un documento da presentare a Consip/AgID su richiesta, con aggiornamento almeno annuale, contenente la valutazione dei rischi inerenti i Centri Servizi e la sicurezza delle informazioni gestite.	Entro 30gg lavorativi dalla stipula del Accordo Quadro e ad ogni successivo aggiornamento
Modulo di reporting per le analisi periodiche di	Predisporre documento di registrazione, da presentare a Consip/AgID su richiesta, degli incidenti rilevati dal proprio personale o da strumenti di monitoraggio a disposizione dei vari servizi della fornitura. Ogni situazione anomala dovrà	Entro 30gg lavorativi dalla stipula del Accordo Quadro e ad ogni

Deliverable	Descrizione	Data di disponibilità
Incidenti, Criticità e Malfunzionamenti	essere registrata e segnalata alle Amministrazioni interessate dai servizi forniti e, laddove necessario, a Consip/AgID, 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.	successivo aggiornamento

4.1.2 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/AgID si riservano 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.
Il Fornitore dovrà effettuare tutte le attività relative alla sicurezza delle informazioni del SGSI in compliance a tale standard. Il Fornitore dovrà predisporre strumenti, processi di gestione e documentazione opportuni a supporto dell'implementazione di quanto previsto contrattualmente.
Consip/AgID si riservano 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 indicare al suo interno almeno i seguenti contenuti:

- illustrare la propria organizzazione che sarà chiamata ad interagire con l'Amministrazione;
- illustrare le modalità con cui garantire la sicurezza delle informazioni da lui gestite e delle strutture di elaborazione delle informazioni oggetto di accessi, elaborate, comunicate a/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, nonché 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 da lui 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 autoeseguibili
  - 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/AgID su richiesta.	Prima consegna alla stipula del Accordo Quadro; successivi aggiornamenti entro 30 gg lavorativi dalla richiesta

5 HELP-DESK

Il Fornitore dovrà garantire e realizzare un servizio di Help Desk, dedicato all'assistenza in remoto, che abbia almeno le caratteristiche minime di seguito indicate.

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

Tale assistenza dovrà riguardare:

- aspetti amministrativi e contrattuali relativi ai Contratti Attuativi 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;
- segnalazione degli incidenti di sicurezza da parte dell'Amministrazione o dal Fornitore; i Referenti tecnici delle Amministrazioni fungeranno da interlocutori con le strutture dell'Help Desk, gestendo al proprio interno il contatto con gli utenti dei servizi;
- segnalazioni 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 dell'Help Desk, gestendo al proprio interno il contatto con gli utenti dei servizi.

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 presente nell'Appendice 1 apposito; un servizio di supporto via e-mail, integrato con il sistema di Trouble Ticketing;
- un'interfaccia web che consenta al referente dell'Amministrazione di inoltrare segnalazioni attraverso il sistema di Trouble Ticketing, sopra indicato in modalità H24.

Il Fornitore dovrà realizzare e/o mettere a disposizione un "Sistema di Trouble Ticketing - TT" per:

- la gestione dei TT aperti proattivamente dal Fornitore stesso;
- la gestione dei TT aperti da CONSIP/AgID e dalle Amministrazioni contraenti;
- la gestione della riassegnazione di TT a strutture tecniche di secondo livello;
- il monitoraggio dello stato di avanzamento dei TT aperti.

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

- codice identificativo del TT;
- 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 TT;
- descrizione della soluzione;
- diagnosi del malfunzionamento, ove applicabile;
- data e orario di chiusura.

6 GESTIONE DEGLI INCIDENTI DI SICUREZZA

In fase di erogazione il Fornitore, al verificarsi di incidenti di sicurezza, dovrà garantire l'attuazione di un processo di gestione (Incident Management) al fine di evitare o minimizzare la compromissione dei dati e dei servizi dell'Amministrazione. Il processo di gestione degli incidenti di sicurezza di seguito descritto si applica in presenza di attivazione del servizio di SOC di cui al paragrafo 3.1.1.

Tale processo, attraverso 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 processo di gestione degli incidenti di sicurezza dovrà inoltre consentire all'Amministrazione il rispetto degli obblighi di quanto indicato dal Regolamento GDPR n. 679/2016 in materia di violazione di dati personali e di 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.

Il processo di gestione degli incidenti di sicurezza dovrà garantire le seguenti fasi:

- segnalazione, 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.

Successivamente alla segnalazione all'Help-desk di un incidente di sicurezza da parte dell'Amministrazione e/o generate in automatico dagli strumenti di monitoraggio e controllo del Fornitore, lo stesso dovrà eseguire il seguente processo di gestione degli incidenti che si compone almeno delle seguenti fasi di seguito riportate.

<u>Identificazione e analisi di un incidente</u>

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". Le operazioni di identificazione devono permettere di verificare, per ogni caso di evento anomalo o sintomo di un incidente, se si è in presenza di un incidente reale di sicurezza.

Tale fase dovrà comprendere:

- 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 "prima investigazione" (di breve periodo) esplicativo dei primi elementi, del livello di gravità e della natura dell'incidente di sicurezza. 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. Il deliverable "prima investigazione" dovrà successivamente essere integrato di tutte le informazioni emerse in fase di completamento dell'attività di investigazione.

<u>Identificazione delle azioni di contenimento relative all'incidente</u>

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 <u>azioni di contenimento di breve periodo</u> 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. Tale

attività dovrà prevedere la trasmissione da parte del Fornitore al referente tecnico dell'Amministrazione del deliverable "azioni di primo contenimento" esplicativo delle azioni di cui 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.

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.

Il deliverable "azioni di primo contenimento" dovrà successivamente essere integrato di tutte le azioni identificate in fase di completamento dell'attività 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.

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:

- 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 (hardening).

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 di gestionali dell'Amministrazione e/o del Fornitore in base alla responsabilità di amministrazione dei sistemi/servizi interessati.

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 SGSI di cui al paragrafo 4.1.1, 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 7.2, e potrà essere adattato, ove richiesto dall'Amministrazione, in relazione alle modalità gestionali della stessa.

7 ATTIVITA' PROPEDEUTICHE

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.
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.

In questo ambito trovano applicazione le regole relative agli indicatori di qualità riportati nell'Appendice 1 Indicatori di Qualità.

7.1 Attività propedeutiche all'erogazione dei servizi

Entro il termine di 15 giorni lavorativi dalla data di stipula di ciascun Contratto esecutivo, il Fornitore dovrà effettuare un'attività di presa in carico, sulla base del Piano di Presa in carico predisposto dal Fornitore in sede di Piano Operativo e all'interno del Piano di lavoro generale, pena l'applicazione delle penali di cui all'Accordo Quadro.

Il Piano di Presa in carico 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, la pianificazione temporale, gli strumenti offerti degli strumenti oggetto di fornitura nonché migliorie offerte (obbligatorio);
- acquisizione del know how del contesto tecnico e funzionale dell'Amministrazione, ove richiesto dalla stessa.

Coerentemente con le caratteristiche offerte dal Fornitore e concordate con l'Amministrazione, il Piano riporterà dettagliatamente:

- Nome, descrizione del servizio/attività;
- prodotti dei servizi/attività;
- le risorse professionali ed il corrispondente impegno in termini di giornate lavorative durante la fase di presa in carico;
- nominativo dei referenti tecnici dei servizi;
- il gantt dei servizi, contenente:
  - date di inizio e fine, previste ed effettive, delle singole attività;
  - date di consegna, previste ed effettive, dei singoli prodotti;
  - date di consegna, previste ed effettive, dei report di conformità alle soluzioni proposte in offerta tecnica;
- ambienti, strumenti, soluzioni, sistemi ed ulteriori migliorie offerte.

Si precisa che tutte le risorse professionali impiegate dal Fornitore nelle attività di presa in carico e tutti i referenti tecnici delle attività dovranno successivamente essere impiegati nell'erogazione dei servizi.

Per le risorse impiegate nei servizi e per tutti i referenti tecnici dovranno essere forniti i relativi Curricula Vitae e le eventuali certificazioni possedute e dichiarate in sede di offerta.

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

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

Il Piano di Presa in carico è soggetto all'approvazione dell'Amministrazione.

In sede di offerta tecnica, il Concorrente potrà illustrare il Piano di Presa in carico proposto, con evidenza delle strategie operative ed organizzative per garantire una rapida ed efficace attivazione dei servizi, nonché della numerosità e skill del personale afferente ai team di lavoro dedicati.

Il mancato rispetto, nel corso dell'esecuzione del singolo contratto esecutivo, delle scadenze riportate nel Piano di Presa in carico comporterà l'applicazione dell'indicatore "SLSC – Slittamento di una scadenza contrattuale" dell'Appendice Livelli di Servizio.
Di seguito vengono descritte in dettaglio le singole fasi del processo complessivo.

7.2 Presa in carico

A partire dalla stipula del Contratto esecutivo il Fornitore dovrà svolgere l'attività di Presa in carico.
Nell'ambito della presa in carico rientrano le seguenti attività:

- configurazione del Portale della Fornitura per il Contratto esecutivo;
- predisposizione e configurazione dei servizi oggetto di fornitura nonché di eventuali strumenti tecnologici offerti;
- condivisione ed eventuale adattamento del processo di gestione degli incidenti;
- predisposizione della documentazione relativa alle modalità di misurazione degli Indicatori di Qualità.

Le attività di Presa in carico dovranno essere avviate entro 5 giorni dalla stipula del Contratto esecutivo ed eseguite secondo le tempistiche concordate con l'Amministrazione nel Piano di Presa in carico.
Ove richiesto dall'Amministrazione, il Fornitore dovrà anche svolgere le attività di seguito indicate e finalizzate:

- all'acquisizione di know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione;
- all'acquisizione degli standard, modalità operative, linee guida e metodologie in uso presso l'Amministrazione, ove presenti.

L'attività potrà consistere, ad esempio, in riunioni di lavoro, rilevazione delle configurazioni in essere sui vari sistemi, esame della documentazione esistente (es. elenco degli asset informatici, catalogo dei sistemi e delle applicazioni, etc.) con assistenza di personale esperto, affiancamento nell'operatività quotidiana condotta dall'eventuale fornitore uscente. Qualora la documentazione disponibile risultasse non aggiornata e/o incompleta, tutto ciò dovrà risultare in modo dettagliato in un verbale attestante il completamento del passaggio di consegne. Tale verbale dovrà essere sottoscritto dai due Fornitori, l'uscente e il subentrante (ovvero tra l'Amministrazione contraente e l'Aggiudicatario) e consegnato all'Amministrazione.

Il Fornitore, durante le attività di Presa in carico dovrà garantire:

- la presenza di tutte le figure coinvolte per l'erogazione dei servizi nonché dovranno essere reperibili e disponibili i Referenti Tecnici;
- la presenza ed il mantenimento nel tempo delle percentuali di personale con le certificazioni e/o credenziali dichiarate in offerta tecnica valide e non scadute;
- la predisposizione di un verbale attestante il completamento della presa in carico da redigere secondo le indicazioni fornite dall'Amministrazione e che dovrà essere sottoscritto dal Fornitore e dall'Amministrazione.

La presa in carico è a totale carico dell'aggiudicatario e pertanto non comporterà oneri aggiuntivi per l'Amministrazione.

L'attività di presa in carico dovrà essere completata entro il termine massimo di 1 mese solare dalla data di stipula del Contratto esecutivo.

Le attività di Presa in carico dovrà essere eseguita dal Fornitore nel rispetto dei tempi contrattualmente indicati pena l'applicazione della penale di cui all'Appendice 1 Indicatori di Qualità.

7.3 Trasferimento Know-how

Il Fornitore dovrà predisporre un Piano di Trasferimento per le attività di passaggio di consegne di fine fornitura (*phase-out*) 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 phase-out, o transizione in uscita, consiste nelle seguenti attività da considerarsi come requisiti minimi:

- "passaggio di consegne" nei quali si gestiscano sistemi delle amministrazioni;
- "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 e previsto in sede di offerta tecnica.

Si fa presente che il trasferimento di know-how potrà essere richiesto anche durante l'erogazione dei servizi nel corso della durata contrattuale, direttamente al personale dell'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: un mese di calendario continuativo 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.
- Predisposizione del Piano di Trasferimento: Il Piano di trasferimento (PTF) è un documento che prevede 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 sarà redatto dal Fornitore e sottoposto all'approvazione dell'Amministrazione almeno tre mesi prima della scadenza del Contratto esecutivo, ovvero entro il mese successivo alla data di comunicazione dell'evento che ne comporterà la cessazione anticipata. Il documento prodotto dovrà essere gestito 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).

Il Piano di trasferimento dovrà prevedere, per le fasi di passaggio della conoscenza e verifica, l'effettuazione di sessioni di lavoro nelle quali i rappresentanti del Fornitore e dell'Amministrazione e/o del Fornitore subentrante esamineranno congiuntamente la documentazione relativa agli oggetti da trasferire.
Al termine di ogni riunione sarà redatto l'apposito verbale dal Fornitore.

Il piano conterrà il dettaglio delle singole riunioni relative a tutte le fasi del progetto di trasferimento. Nella redazione del PTF occorre tener conto delle priorità, delle scadenze istituzionali e degli adempimenti tecnico amministrativi dell'Amministrazione.
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 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.
Nel caso in cui l'Amministrazione fruisca di analoghi servizi preesistenti, il Fornitore dovrà esplicitamente prevedere, congiuntamente con l'Amministrazione contraente, le procedure di attivazione necessarie a garantire il mantenimento dell'operatività durante le fasi di migrazione. Eventuali necessità di fermo dei servizi devono essere accuratamente definite dal Fornitore, approvate dall'Amministrazione e monitorate in modo da ridurre al minimo gli impatti sull'utenza di riferimento.
Si precisa inoltre che in fase di avvio dell'erogazione dei servizi, il Fornitore dovrà sottoscrivere un accordo di riservatezza che lo impegna a non divulgare nessuna informazione relativa all'Amministrazione contraente, alle sue infrastrutture informatiche e ai suoi dati.

7.5 Eventuali attività di installazione per l'erogazione dei servizi

In relazione ad eventuali attività di installazione/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 intervalli orari definiti dall'Amministrazione contraente, 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 per collaudo eseguito con esito positivo.

7.6 Eventuali attività di migrazione funzionali alla presa in carico dei servizi

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 dei Servizi specialistici di cui al paragrafo 1.1.1.30; 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.

7.7 Team 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 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 Portale della fornitura, il Fornitore dovrà pubblicare i CV delle risorse proposte (ivi compresi i Referenti tecnici ed i ruoli aggiuntivi proposti), con la documentazione comprovante le eventuali competenze e certificazioni possedute e dichiarate in sede di offerta tecnica.

Per l'accettazione del personale proposto, 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 personale essa procederà alla richiesta formale di sostituzione, anche nel periodo di Presa in carico.

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**
Pubblicazione sul Portale dei CV risorse PRESA IN CARICO e dei referenti tecnici	Stipula	5 giorni lavorativi	Allegato al piano di PRESA IN CARICO
Pubblicazione sul Portale dei CV delle risorse professionali e dei ruoli di interfaccia con l'Amministrazione	Stipula	10 giorni lavorativi	Allegato al piano di lavoro generale

Vincoli temporali			
Attività	**Evento**	**Giorni**	**Note**
Colloquio	Richiesta di colloquio	3 giorni lavorativi	
Disponibilità della risorsa nei team di lavoro	Comunicazione dell'esito positivo del colloquio	3 giorni lavorativi	In funzione degli specifici piani approvati
Pubblicazione sul Portale dei CV 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

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 dall'Amministrazione.

7.8 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 le competenze, le conoscenze e le relative certificazioni/credenziali delle risorse professionali che dovranno essere impiegate dal Fornitore per l'esecuzione della fornitura.

8 MODALITÀ DI EROGAZIONE

8.1 Comunicazioni e Approvazioni

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

Per favorire l'agilità e la digitalizzazione dei processi – a partire da quelli interni di interazione con l'Amministrazione – il Fornitore dovrà rendere disponibile sul Portale della fornitura una apposita funzione di validazione dei documenti e di approvazione da parte dell'Amministrazione.
Il ciclo di vita dei documenti ufficiali dovrà essere definito nel Piano della Qualità Generale e verificabile nella Prima Release del Portale.

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.

8.2 Modalità di Approvazione

Tutte le comunicazioni inerenti l'approvazione (o mancata approvazione) dei prodotti della fornitura saranno notificati tramite il Portale. 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
- Piano di migrazione, ove previsto
- Piani di lavoro di ciascun servizio;
- Piano di trasferimento di know-how;
- 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 della Amministrazione, che pertanto potrà non accettarli e richiedere di apportare le modifiche ritenute necessarie.

Per i servizi oggetto di fornitura, nel caso si verifichino 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 Amministrazione.

8.3 Verifiche di conformità

Il soggetto deputato all'esecuzione delle attività di verifica di conformità, dopo aver acquisito la documentazione tecnico-funzionale dei servizi (sia a carattere continuativo che a consumo), procederà a verificare la corretta esecuzione degli stessi.

8.4 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.
Pertanto, 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.

8.4.1 Rilievi

I rilievi sono le azioni di avvertimento da parte della Amministrazione conseguenti il non rispetto delle indicazioni contenute nella documentazione contrattuale. Pertanto 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 alla Amministrazione un documento con elementi oggettivi ed opportune argomentazioni entro 3 giorni lavorativi dall'emissione del rilievo.

8.4.2 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) dalla Amministrazione al corrispettivo da erogarsi che è stabilito per prestazioni effettuate nel rispetto dei requisiti.

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

8.5 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 dalla 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 della Amministrazione, di strumenti automatici a ciò deputati.

Il Fornitore si impegna ad inviare alla 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.

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

8.6 Team di Lavoro

Il Fornitore, per l'erogazione dei servizi che prevedono Team di Lavoro, dovrà disporre delle competenze, esperienze e capacità richieste ai profili professionali indicati di seguito, che devono tutte **obbligatoriamente** fare parte dei Team di Lavoro (o Team Ottimale) di ciascun servizio.

I Team di Lavoro sono sotto la responsabilità e l'organizzazione del Fornitore che ha la responsabilità di strutturare i migliori gruppo di lavoro in funzione dell'operatività e dei deliverable richiesti, garantendo la disponibilità dei profili professionali e delle competenze previste.

I Profili Professionali previsti nei Team sono i seguenti (per il dettaglio dei profili si rimanda all'Appendice 2 Profili Professionali):

- Security Principal
- Senior information security consultant
- Junior information security consultant
- Security solution architect

La tariffa offerta per il servizio in giorni persona si riferisce al Giorno Team Ottimale (pari a 8 ore lavorative). L'importo del servizio è determinato sulla base dei giorni/team definiti dall'Amministrazione nel Piano dei Fabbisogni.

Il Fornitore sarà libero di organizzare le suddette figure nell'ambito del proprio Team Ottimale in autonomia per soddisfare le richieste progettuali dell'Amministrazione, garantendo in ogni caso il rispetto delle scadenze previste, degli indicatori di qualità ed il livello atteso dei deliverables di fornitura.
Ai fini della remunerazione a corpo, il Fornitore sarà libero di organizzare le suddette figure nell'ambito del proprio "team ottimale" per singolo servizio. L'Amministrazione in ogni caso avrà la possibilità, nella fase di esecuzione dei servizi, di verificare l'effettiva presenza di tali figure nel team di lavoro dedicato all'erogazione dei servizi.

Le certificazioni e le competenze richieste ed offerte dovranno risultare aggiornate alle ultime versioni per tutta la durata dell'Accordo Quadro.

8.7 Dimensionamento dei servizi

8.7.1 Progettuale (a corpo)

Per i servizi con dimensionamento progettuale (a corpo) 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.

Il Fornitore sulla base dei requisiti, declina le caratteristiche del servizio, gli obiettivi e tutti gli elementi del piano di lavoro, il dettaglio dei prodotti, le stime ed i conteggi, fornendo tutti gli elementi per oggettivare la proposta di servizio ed i relativi costi.

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 inoltre risponderà dei danni causati da errata allocazione delle risorse o incompetenza delle risorse, mancata comprensione delle richieste dell'Amministrazione, mancato rispetto delle linee guida tecnologiche e dei livelli di qualità, ecc., e, dovrà rimediare a proprie spese per erogare una prestazione conforme funzionalmente e tecnicamente ai requisiti approvati.

8.7.2 Continuativa (a canone)

Per i servizi con dimensionamento a canone 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.

Il Fornitore sulla base dei requisiti, declina le caratteristiche del servizio, gli obiettivi e tutti gli elementi del piano di lavoro, il dettaglio dei prodotti, le stime ed i conteggi, fornendo tutti gli elementi per oggettivare la proposta di servizio ed i relativi costi.

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 "fasce incrementali" (es., fascia 1: utenti da 1 a 250; fascia 2: utenti da 251 a 500 ecc..) sono remunerati attraverso l'applicazione del prezzo unitario della fascia corrispondente alla quantità complessiva acquistata. Tale modalità trova applicazione anche per il servizio in modalità a consumo.

8.8 Pianificazione e Consuntivazione

8.8.1 Piano della Qualità Generale

Il Piano della Qualità Generale 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 pubblicare sul Portale i Rapporti sul rispetto del Piano di Qualità della fornitura ed i Rapporti di conformità su tutti gli impegni assunti in offerta tecnica.

8.8.2 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.

1. Descrizione specifica del Contratto esecutivo

2. Scopo del Piano della Qualità

(elenca le motivazioni e le peculiarità dell'obiettivo dell'Amministrazione per le quali è richiesto il documento)

3. Documenti applicabili e di riferimento
4. Ruoli e Responsabilità di riferimento
5. Modalità di erogazione, consuntivazione dei servizi
6. 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)

7. 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)

8. 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).

8.8.3 Piani di Lavoro

Il Fornitore dovrà predisporre, con le tempistiche indicate nel Capitolato Tecnico Generale, e mantenere costantemente aggiornata la pianificazione dei servizi, con la seguente articolazione:

Piano di lavoro generale comprensivo di:

- piano di Presa in carico 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 pubblicherà sul Portale 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 ripubblicando sul Portale 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.

8.8.4 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 progettuali, la frequenza minima di aggiornamento è di 2 settimane, salvo diverso accordo con l'Amministrazione. Per le attività continuative la frequenza minima di aggiornamento è mensile.

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

8.9 Orario di erogazione dei servizi

Nel Piano di fabbisogni l'Amministrazione indicherà l'orario di riferimento e le caratteristiche dei servizi laddove applicabili.

Tabella Orario di erogazione dei servizi

Ambito dei Servizi	Orario
Impiego delle figure professionali per servizi "on-site" (Servizi di Formazione e security awareness e Servizi Specialistici)	Lunedi – Venerdi: 08:30 – 17:30 Sabato (festivi esclusi): 08:30 – 13:30
Help Desk - ricezione richieste tramite operatore Help Desk – ricezione richieste tramite canale Web/mail	Lunedi – Venerdi: 08:30 – 17:30 Sabato (festivi esclusi): 08:30 – 13:30 H24, 7 gg su 7
Disponibilità, monitoraggio e gestione incidenti dei servizi da remoto; Gestione degli incidenti di sicurezza.	H24, 7 gg su 7

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.

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;
- in caso sia presente un team di lavoro l'orario sarà garantito secondo una distribuzione delle presenze, eventuale turnazione delle risorse a copertura dell'intero orario, da concordare con l'Amministrazione nel piano di lavoro. All'interno dell'orario di servizio, non sono previste maggiorazioni;
- relativamente all'extraorario pianificato (oltre le ore 17,30 – dal lunedì al venerdì ed oltre le ore 14:00 il sabato) nonché domenica e festivi, gli interventi (on-site o da remoto) verranno retribuiti alla tariffa oraria base maggiorata del 20%;
- 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 oraria è data dalla tariffa giornaliera offerta (riferita a 8 ore lavorative) diviso 8.

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 disponibilità alla richiesta di estensione dell'orario di servizio suddetto è da considerare già remunerata nel corrispettivo globale della fornitura.
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 il sabato, la domenica e/o nei giorni festivi: 8 ore lavorative.

L'amministrazione potrà richiedere l'estensione dell'orario di servizio attraverso il Portale della fornitura o via posta elettronica. Il Fornitore dovrà accettare la richiesta se pervenuta nel periodo di preavviso prestabilito.

I volumi di attività da effettuarsi in extra orario 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 esteso.

Le Amministrazioni potranno sottoporre al Comitato di coordinamento e controllo eventuali richieste per ulteriori esigenze in termini di orario di servizio.