



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

**CAPITOLATO TECNICO SPECIALE
LOTTI 3 E 4**

Classificazione Consip: Ambito pubblico

Indice

1.	SCOPO DEL DOCUMENTO	4
2.	OGGETTO	4
3.	DESCRIZIONE DEI SERVIZI	5
3.1.	Lx.S13 - Security Governance	6
3.2.	L1.S14 - Formazione e Security awareness	9
3.3.	Lx.S15 - Supporto alla definizione dei processi cyber	13
3.4.	Lx.S16 – Cyber Risk Management	15
3.5.	Lx.S17 - Compliance normativa	17
3.6.	Lx.S18 - Vulnerability assessment	20
3.7.	Lx.S19 - Penetration testing	23
3.8.	Lx.S20 - Analisi del codice - statico	25
3.9.	Lx.S21 - Analisi del codice - dinamico	27
3.10.	Lx.S22 - Analisi del codice - mobile	31
3.11.	Lx.S23 – Controllo terze parti (supply-chain di approvvigionamento)	32
3.12.	Modalità di erogazione in configurazione ibrida o on-premise	35
4.	REQUISITI DI ESECUZIONE	36
4.1.	ISO 9001	36
4.2.	ISO 27001	36
4.3.	DNSH	37
5.	FASI OPERATIVE DELLA FORNITURA	38
5.1.	Presa in carico e startup	38
5.2.	Modalità di attivazione dei servizi	39
5.3.	Fine fornitura	40
5.4.	Exit Strategy e Grace Period	41
6.	MODALITÀ DI EROGAZIONE	42
6.1.	Risorse da impiegare nell'affidamento dei servizi	42
6.2.	Competenze richieste	43
6.3.	Comunicazioni e Approvazioni	44
6.4.	Modalità di Approvazione	44
6.5.	Verifiche di conformità	45
6.6.	Azioni contrattuali	45
Rilievi	45	
Penali	46	
6.7.	Monitoraggio	46
Reportistica e strumenti di monitoraggio		46
6.8.	Dimensionamento dei servizi	47
6.9.	Pianificazione e Consuntivazione	49

1. SCOPO DEL DOCUMENTO

Il presente capitolato è parte integrante della documentazione di gara e definisce le caratteristiche e i requisiti per l'affidamento dei servizi di Governance, Analisi del Rischio e Controllo (GRC) in ambito Sicurezza informatica per le Pubbliche Amministrazioni.

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

Ciò comporta che:

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

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

Appendice 1 – Indicatori di Qualità - Lotti 3 e 4;

Appendice 2 – Profili Professionali - Lotti 3 e 4.

2. OGGETTO

Relativamente ai **Lotti 3 e 4**, l'oggetto della fornitura comprende i servizi indicati nella seguente tabella:

ID Servizio	Servizio
Lx.S13	Security Governance
Lx.S14	Awareness e Formazione
Lx.S15	Supporto alla definizione processi cyber
Lx.S16	Cyber Risk Management
Lx.S17	Compliance normativa
Lx.S18	Vulnerability Assessment
Lx.S19	Penetration Testing
Lx.S20	Analisi del codice – Statico
Lx.S21	Analisi del codice – Dinamico
Lx.S22	Analisi del codice – Mobile
Lx.S23	Controllo terze parti (supply-chain di approvvigionamento)

Tabella 1 – Elenco servizi

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

- Lx; ove x è l'identificativo del numero del Lotto che può assumere valore 3 o 4;
- Sn; ove n è il numero progressivo del Servizio.

3. DESCRIZIONE DEI SERVIZI

I servizi di Governance, Analisi del Rischio e Controllo hanno l'obiettivo di mettere a disposizione dell'Amministrazione risorse professionali e tecnologie finalizzati alla definizione e attuazione di una "strategia di cyber sicurezza" ovvero all'insieme di misure da adottare finalizzate alla identificazione dello stato di sicurezza del sistema informativo e alla sua protezione. La strategia di cyber sicurezza dovrà pertanto consentire all'Amministrazione di:

- identificare il livello iniziale di vulnerabilità delle componenti infrastrutturali ed applicative del proprio sistema informativo;
- definire una strategia di governance della sicurezza informatica inerenti gli aspetti tecnologici, organizzativi e normativi;
- dare attuazione alle misure di sicurezza di cui alle linee guida ACN per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90 e relativi impianti documentali;
- supportare l'Amministrazione nella fase di definizione dei processi e procedure operative per la gestione degli incidenti informatici;
- adottare la "tassonomia cyber" (TC-ACN) definita da ACN disponibile al link <https://www.csirt.gov.it/contenuti/la-tassonomia-cyber-dellacn>;
- identificare le esigenze in termini di fabbisogni di beni/servizi di sicurezza di cui l'Amministrazione per attuare le misure di difesa ed in particolare relativamente ai servizi dei Lotti 1 e 2;
- esercitare una azione di controllo imparziale sulla corretta esecuzione dei servizi di sicurezza dei Lotti 1 e 2 e sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

Mediante l'utilizzo dei servizi oggetto di fornitura dei Lotti 3 e 4, il Fornitore dovrà quindi supportare l'Amministrazione nell'organizzazione, pianificazione, analisi, misura e controllo nonché di coordinamento generale per la verifica tecnica e organizzativa di attuazione delle misure sicurezza intraprese.

Il Fornitore sarà chiamato ad erogare i servizi oggetto di fornitura in funzione delle esigenze dell'Amministrazione, garantendo la messa a disposizione di risorse professionali, strumenti e tecnologie, metodologie e supporti.

A tal fine è di fondamentale importanza che il Fornitore si interfacci efficacemente con le strutture interne dell'Amministrazione, in modo da poter concretizzare la strategia di cyber security adottata, supportare il raggiungimento di obiettivi complessivi.

Il Fornitore dovrà erogare i servizi tenendo conto del contesto normativo e organizzativo dell'Amministrazione beneficiaria, nonché delle sue specificità dimensionali e tecnologiche. Inoltre, data la rilevanza e la complessità delle tematiche oggetto dei servizi, è richiesta disponibilità, dinamicità, accuratezza e riservatezza nell'esecuzione dei servizi.

Considerata la natura strategica dei servizi, gli stessi dovranno essere erogati da personale esperto, con elevato grado di specializzazione e con una profonda conoscenza del contesto della cyber sicurezza.

Il Fornitore dovrà garantire la totale copertura dei fabbisogni dell'Amministrazione, anche in situazioni di particolare urgenza o complessità, prevedendo la totale flessibilità e puntualità nell'impiego delle risorse professionali per l'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 adeguatezza e conformità della documentazione e degli elaborati prodotti.

Le attività condotte saranno oggetto di preventiva condivisione e di successiva approvazione da parte dell'Amministrazione, anche nell'ambito delle finalità di monitoraggio della qualità.

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

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

Il Fornitore si impegna a rilasciare ogni deliverable nel formato richiesto dall'Amministrazione.

La modalità di esecuzione dei servizi è principalmente di tipo **“on-site”**: presso le sedi dall'Amministrazione, ove dalla stessa indicate; in alternativa presso la sede del Fornitore.

3.1. Lx.S13 - Security Governance

Requisiti tecnico-funzionali del servizio

Il servizio di Security Governance dovrà fornire all'Amministrazione un supporto volto a definire la strategia di cyber sicurezza, individuare e monitorare le relative azioni strategiche adottate.

Di seguito sono proposti gli ambiti di intervento del servizio di Security Governance che il fornitore dovrà garantire.

a) Supporto dell'Amministrazione nella definizione e controllo delle scelte strategiche inerenti al governo della sicurezza delle informazioni, degli indirizzi organizzativi, tecnologici e dell'approccio da adottare a fronte di nuovi paradigmi architettureali, scenari di attacco e situazioni di rischio consolidate.

In particolare, il servizio potrà riguardare specifici temi di interesse dell'Amministrazione, di cui a titolo esemplificativo e non esaustivo, consulenza e supporto volti alla:

- identificazione, attuazione e controllo delle linee strategiche cyber dell'Amministrazione che tengano in considerazione almeno i seguenti ambiti, quali:
 - “Governance” degli asset e dei processi;

- “Management” ovvero gestione della continuità operativa (network, application, content, data center, identity);
 - “Risk” ovvero gestione del rischio di esposizione e mitigazione;
 - “Awareness” degli utenti verso i rischi di sicurezza;
 - “Incident” ovvero processi, soluzioni e governance centralizzata delle infrastrutture critiche;
 - “Compliance” normativa.
- Identificazione dell’approccio alla cybersecurity dell’organizzazione definendo, ad esempio, piani strategici in linea con gli obiettivi dell’organizzazione in termini di sicurezza dei propri sistemi informativi e di rete.
 - verifica costante di allineamento della strategia cyber dell’Amministrazione con le linee guida, le direttive e normative a livello nazionale ed europeo e supporto alla PA alle attività correlate agli obblighi imposti dalle stesse (ad esempio segnalazioni, monitoraggio, etc);
 - identificazione e controllo delle iniziative in materia di sicurezza informatica e sicurezza delle informazioni anche in funzione dell’introduzione di nuovi elementi infrastrutturali, organizzativi, applicativi all’interno del contesto di riferimento dell’Amministrazione;
 - valutazione degli impatti e dei rischi inerente i contratti di servizio in essere dell’Amministrazione, relativi a problematiche di sicurezza;
 - indirizzo e controllo della coerenza complessiva delle iniziative di sicurezza informatica e sicurezza delle informazioni, in funzione delle “lesson learned” derivanti dalla gestione di incidenti di sicurezza, risultati di audit interni, security assessment periodici;
 - adeguamento, evoluzione e controllo della strategia di sicurezza, delle architetture e delle tecnologie dell’Amministrazione, in relazione al modello IT adottato;
 - definizione di studi di fattibilità e analisi d’impatto di tipo tecnico ed organizzativo in materia di sicurezza informatica volti a supportare le scelte di evoluzione del modello IT e gli impatti di tipo cyber (on- premise, cloud, ibrido, multicloud, OT/XIoT) dell’Amministrazione;
 - supporto dell’Amministrazione nel processo di trasformazione digitale, di trasformazione della tecnologia dell’IT e della cyber sicurezza;
 - formulazione di una strategia e di una architettura di monitoraggio valutando lo stato corrente della gestione dei sistemi, persone, partner, outsourcing, strumenti, complessità, gap e rischi dell’Amministrazione;
 - definizione, manutenzione e consolidamento delle tassonomie e delle classificazioni in materia di sicurezza informatica (es. tassonomia e classificazione incidenti, classificazione degli asset, ecc.);
 - definizione degli elementi di base inerenti il processo di gestione della sicurezza e delle informazioni (definizione del rischio accettabile, identificazione delle minacce e degli elementi di applicabilità ai contesti di riferimento, ecc.);

- supporto alle attività decisionali delle strutture di vertice ICT dell'Amministrazione in materia di cyber sicurezza;
- partecipazione a gruppi di lavoro, comitati, tavoli di coordinamento, per la definizione delle linee strategiche, l'analisi delle esigenze e la produzione di documentazione;
- monitoraggio della conduzione e reporting dei risultati dell'attività.

b) Supporto nella definizione delle scelte strategiche inerenti l'identificazione dei fabbisogni di beni e servizi in materia di ICT Security.

In particolare, il servizio potrà riguardare specifici temi di interesse dell'Amministrazione, di cui a titolo esemplificativo e non esaustivo, consulenza e supporto volti alla:

- predisposizione di studi e analisi di mercato volte alla copertura dei fabbisogni di beni e di servizi per la gestione della sicurezza ICT in una prospettiva di breve e medio termine in coerenza con il contesto tecnologico/organizzativo dell'Amministrazione, le scelte di strategie di evoluzione adottate e gli obiettivi attesi nonché in relazione agli scenari di rischio del contesto di riferimento;
- supporto all'elaborazione del piano annuale degli acquisti in materia di sicurezza informatica dell'Amministrazione;
- supporto all'Amministrazione nella fase di analisi e valutazione delle stime quantitative ed economiche relative a servizi di sicurezza oggetto di acquisizione;
- supporto all'Amministrazione nell'organizzazione, pianificazione, controllo nonché di coordinamento generale per la verifica di esecuzione dei servizi di sicurezza erogati da remoto in favore della stessa;

Ove richiesto, il Fornitore dovrà:

- coadiuvare l'Amministrazione per la raccolta dei dati qualitativi e quantitativi per la rappresentazione degli elementi di fornitura e la definizione delle caratteristiche di dettaglio necessarie alla predisposizione del Piano dei Fabbisogni;
- verificare la completezza del documento di Contesto Tecnologico ed Applicativo, parte integrante del Piano stesso;
- supportare l'Amministrazione nella verifica tecnico-economica del Piano Operativo presentato dal Fornitore dei Lotti 1 e 2 dei servizi Managed Security Services;
- supportare l'Amministrazione nella verifica di tutti gli elementi costitutivi della proposta del Fornitore dei Lotti dei servizi di sicurezza da remoto inserita nel Piano Operativo, coerentemente con quanto già offerto in AQ;
- supportare l'Amministrazione nell'elaborazione della richiesta di eventuali modifiche e/o integrazioni da apportare al Piano dei fabbisogni e del Piano Operativo.

Figure professionali

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

- Security Principal;
- Security Solution Architect;
- Information Security Consultant Senior;
- Information Security Consultant Junior;
- Cloud Security Expert;
- OT/IoT Security Expert;
- Data Protection Specialist.

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

Metrica di dimensionamento e modalità di remunerazione

Per ciascuna figura professionale è prevista:

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

La metrica di dimensionamento del servizio "Security Governance" è: **Giorno/Persona**.

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

3.2. L1.S14 - Formazione e Security awareness

Requisiti tecnico-funzionali del servizio

Il servizio "Formazione e Security awareness" è mirato a sensibilizzare l'Amministrazione sul tema della sicurezza informatica, 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 gli incidenti di sicurezza e reagire al meglio a fronte di eventuali problemi.

Il servizio, in coerenza con il Decreto Legislativo 4 settembre 2024, n. 138 (recepimento direttiva NIS 2), dovrà consentire l'acquisizione di conoscenze e competenze al personale dell'Amministrazione al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività dell'Amministrazione.

Si riportano a titolo esemplificativo e non esaustivo alcuni ambiti connessi alle minacce Cyber di interesse per gli utenti che possono essere oggetto di formazione specifica:

- Phishing;
- Password,
- Social Media,
- Privacy & GDPR,
- Mobile & App,
- Fake News,
- USB Device,
- E-mail Security,
- Malware & Ransomware,
- Web Browsing,
- Servizi cloud
- Social Engineering, Clean Desk,
- Smart Working,
- Social Collaboration & Video Conferenze,
- Ransomware,
- Multi Factor Authentication,
- IoT Device,
- Bluetooth & WiFi,
- Classificazione delle Informazioni,
- Data Protection,
- Cyberbullismo,
- Aspetti legali,
- Sicurezza Fisica,
- Backup & Restore (per gli utenti).

Dovranno essere disponibili modalità di formazione 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, quali ad esempio:

- **formazione sincrona:** tipicamente workshop formativi in presenza o da remoto;
- **formazione asincrona,** basato su moduli didattici, suddivisi a loro volta in video pillole fruibili in modalità e-Learning;
- **addestramento esperienziale** automatizzato multicanale (campagne di phishing, smishing, QRcode, memorie USB), basato su simulazioni di attacco;
- **addestramento didattico induttivo** costituito da episodi video di tipo narrativo che, seguendo un metodo di formazione per immedesimazione, coinvolgono l'utente in

situazioni realistiche di concretizzazione delle minacce Cyber, sviluppando un naturale processo di autoidentificazione.

Il fornitore dovrà inoltre supportare l'Amministrazione:

- nella definizione dei **fabbisogni formativi** in ambito Cybersecurity & Digital Protection della popolazione target (es. intera popolazione, personale tecnico, dirigenza ecc.);
- nell'attuazione di **piani di studi**, modulabili in funzione dei target di partecipanti e delle esigenze della PA, con verifica della propedeuticità, per cui è necessario completare con successo una lezione, per passare alla successiva al fine di raggiungere il grado minimo necessario di comprensione dei temi proposti prima di passare ai temi successivi. Ripetibilità dei test per non costituire un blocco assoluto all'avanzamento;
- **nel mantenimento delle conoscenze** per gli utenti che hanno già raggiunto un livello di conoscenza e per i quali è fondamentale attivare un processo di mantenimento delle competenze e conoscenze acquisite, attraverso l'impiego di metodologie basate su teorie dell'apprendimento e opera impiegando oggetti formativi interattivi (Escape Room, DidActive, Cyber Game, ecc.) che generano feedback di "rinforzo" quando l'interazione è corretta e di "riorientamento" quando l'interazione è errata o parzialmente scorretta.

Tra le caratteristiche del modello formativo dovranno essere previsti:

- la funzione di **gamification** quale driver di rafforzamento dei meccanismi di apprendimento mediante il coinvolgimento degli utenti sulla base di logiche, meccaniche ed elementi tipici dei giochi.
- **l'aderenza linguistica** e culturale al contesto dell'utente con sviluppo dei contenuti nativamente in italiano, rendendo così naturale l'apprendimento rispetto a quanto avviene con l'impiego di contenuti con uno stile fortemente anglosassone. Possibilità di trasposizioni nelle principali lingue europee e intercontinentali tramite traduttori madrelingua almeno inglese, francese e spagnolo;
- l'utilizzo di tecniche di **verifica dei livelli di apprendimento** raggiunti dai fruitori dei corsi in parallelo con l'avanzamento del programma formativo, con l'obiettivo di misurare costantemente il livello di conoscenza raggiunto da ogni utente e sollecitare la risoluzione delle lacune per gli utenti che risultino più deboli;
- l'utilizzo di **cruscotti di gestione** unificati, mediante dashboard di gestione della formazione, degli utenti e di accesso alla reportistica.
- **la fruibilità** da qualsiasi dispositivo (PC, Tablet, Smartphone) e dai più diffusi Browser Internet;

- la somministrazione di questionari di **rilevazione del gradimento**, anche con format eventualmente forniti dalla Committente, e provvedere alla relativa analisi dei dati rilevati. Il set minimo di elementi oggetto di valutazione dovrà includere:
 - qualità del docente;
 - efficacia dell'intervento formativo;
 - metodologia didattica
 - programma e argomenti;
 - materiale didattico;
 - eventuali commenti dei discenti.

Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento del servizio "Formazione e Security awareness" è: **Modulo formativo.**

La modalità di remunerazione del servizio di "Formazione e Security awareness" è: **a consumo.**

3.3. Lx.S15 - Supporto alla definizione dei processi cyber

Requisiti tecnico-funzionali del servizio

Il servizio "Supporto alla definizione degli processi cyber" dovrà prevedere all'Amministrazione, il supporto alla definizione delle attività di definizione dei processi e procedure in ambito cyber sicurezza ed in particolare degli aspetti di analisi degli incidenti cyber e di divulgazione delle informazioni in caso di emergenza.

In particolare, potrà prevedere:

- la creazione e gestione di un piano di risposta agli incidenti (IRP);
- l'investigazione e analisi degli incidenti;
- la verifica continuativa dei preallarmi, allerte, bollettini e delle informazioni in merito a rischi e incidenti emessi dal CSIRT-Italia;
- l'identificazione della remediation dell'incidente;
- l'analisi dei log e degli eventi;
- il malware forensic;
- il network e system forensic;
- il supporto ai processi di escalation verso le entità interne ed esterne (ACN, CSIRT Italia, organi di polizia giudiziaria);
- il supporto alla gestione delle comunicazioni interne/esterne e degli aggiornamenti durante o immediatamente dopo gli incidenti;
- le raccomandazioni post-incidente.

Si riportano di seguito, a titolo indicativo e non esaustivo, le attività di supporto organizzativo del servizio:

- supporto nella incident management strategy, ossia definizione delle modalità di gestione degli incidenti informatici, delle azioni di contenimento nell'ambito dei processi dell'Amministrazione, gestione del rapporto con le entità interne ed esterne, in coerenza con le prassi e gli standard emessi del CSIRT Italia;
- supporto nella definizione di procedure di Log Management per la raccolta, archiviazione e analisi dei dati di log;
- supporto alle Amministrazioni per il recepimento e la conformità alle prescrizioni organizzative della normativa di settore (Legge 28 giugno 2024, n. 90, direttiva NIS 2) per le attività di notifica degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti;
- supporto nella progettazione, gestione ed evoluzione del monitoraggio in termini di definizione degli use-case relativi negli incidenti di sicurezza, supporto alla progettazione delle regole di correlazione e validazione dei sistemi/servizi di rilevazione in essere dell'Amministrazione;
- supporto alla definizione dei processi di tuning dei sistemi/servizi di rilevazione degli allarmi di sicurezza dell'Amministrazione;

- supporto all'Amministrazione nell'organizzazione, pianificazione, controllo nonché di coordinamento generale per la verifica tecnica di esecuzione di sicurezza erogati da remoto in favore all'Amministrazione, con particolare attenzione alle attività di verifica dei risultati attesi. Nell'esecuzione del servizio il Fornitore dovrà operare in coerenza con le previsioni indicate nelle Linee Guida Agid; in particolare si citano le Linee guida per lo sviluppo del software sicuro nella pubblica amministrazione (allegati tecnici 1, 2, 3 e 4).

Figure professionali

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

- Security Principal;
- Information Security Consultant Senior;
- Information Security Consultant Junior;
- Forensic Expert.

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

Metrica di dimensionamento e modalità di remunerazione

Per ciascuna figura professionale è prevista:

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

La metrica di dimensionamento del servizio di "Supporto alla definizione dei processi cyber" è: **giorni/persona**.

La modalità di remunerazione del servizio di "Supporto alla definizione dei processi cyber" è: **a tempo/spesa oppure a corpo**.

3.4. Lx.S16 – Cyber Risk Management

Requisiti tecnico-funzionali del servizio

Il servizio “Cyber Risk Management” dovrà supportare l’Amministrazione nella analisi, valutazione e gestione del rischio informatico al fine di individuare potenziali vulnerabilità che possono mettere a rischio la sicurezza dei dati dell’organizzazione e per la definizione e aggiornamento dei piani di continuità operativa (Business Continuity e Disaster Recovery).

Si considerano le seguenti categorie di rischio:

1. cyber crime, ovvero le attività illegali commesse tramite differenti tecniche d’attacco (quali il ransomware ed il social engineering);
2. il rischio IT “puro”, rappresentato da eventi accidentali sui sistemi IT (incendi, blackout elettrico, errore umano ecc.);

In risposta al punto 1, il fornitore dovrà garantire:

- la messa a disposizione di una piattaforma di Risk Management, senza oneri aggiuntivi per l’Amministrazione. Nel caso in cui l’Amministrazione disponga già di una propria piattaforma di Risk Management e non intenda utilizzare quella messa a disposizione del Fornitore, il Fornitore stesso dovrà erogare il servizio utilizzando la piattaforma dell’Amministrazione.
- il supporto nella identificazione, quantificazione e prioritizzazione di qualsiasi rischio cyber esistente prendendo in considerazione gli specifici contesti organizzativi (es. infrastrutture critiche), minacce applicabili (ad esempio, ransomware, minacce avanzate e persistenti) e vincoli normativi al fine di garantire decisioni strategiche e allocazioni di budget basate sull’approccio risk based;
- l’utilizzo di un framework e linee guida per la gestione del rischio di cybersecurity, in conformità a normative e standard di riferimento, e lo svolgimento delle fasi di:
 - Definizione del contesto,
 - Risk assessment;
 - Risk identification;
 - Risk analysis;
 - Risk evaluation;
 - Risk treatment;
- la definizione e il monitoraggio dei piani di remediation;
- l’analisi e consolidamento delle pratiche di gestione della qualità e del rischio dell’organizzazione della PA;
- il supporto agli owner degli asset aziendali, ai dirigenti e agli altri stakeholder nella fase di decisione sui rischi per gestirli e mitigarli;
- l’elaborazione, presentazione e consegna alla PA di reportistica e deliverable, quali ad esempio:
 - Analisi del contesto

- Report di Assessment
- Risk assessment
- Procedure di riferimento per gli Standard (es. Manuale Operativo)
- Remediation Plan
- Gantt e Roadmap di realizzazione degli interventi
- Risk Management Executive Summary

In risposta al punto 2, il fornitore dovrà garantire l'elaborazione e il mantenimento di piani di continuità operativa, comprensivi della Business Impact Analysis, che delinea come una organizzazione potrà continuare ad operare durante un'interruzione non pianificata del servizio, comprendendo piani di emergenza per i processi aziendali, gli asset, le risorse umane e i partner commerciali e ogni aspetto del business che potrebbe essere colpito.

In particolare, si indica a titolo esemplificativo e non esaustivo:

- la definizione dei processi strategici a rischio, la conseguente dipendenza dai sistemi IT e i risultati della valutazione del rischio;
- la valutazione delle conseguenze di possibili eventi di crisi e l'identificazione delle funzioni organizzative chiave;
- l'impatto sul business, ovvero l'identificazione delle funzioni più critiche in base ai costi che avranno sull'intero business (sanzioni legali, interruzione dei servizi, insoddisfazione degli utenti, cittadini, ecc.);
- l'analisi dei tempi relativi allo stato di crisi, valutato per calcolare il Recovery Point Objective (RPO) e il Recovery Time Objective (RTO) e il Maximum Allowable Downtime (MAD);
- la definizione del piano di continuità;
- la definizione dei test di disaster recovery e il supporto al monitoraggio della continuità operativa;
- la gestione della crisi, supporto all'attuazione del piano di continuità.

Figure professionali

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

- Risk Manager;
- Security Manager;
- Security Auditor Senior;
- Information Security Consultant Senior;
- Information Security Consultant Junior;
- Data Protection Specialist.

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

Metrica di dimensionamento e modalità di remunerazione

Per ciascuna figura professionale è prevista:

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

La metrica di dimensionamento del servizio di “Cyber Risk Management” è: **giorni/persona**.

La modalità di remunerazione del servizio di “Cyber Risk Management” è: **a tempo/spesa** oppure **a corpo**.

3.5. Lx.S17 - Compliance normativa

Requisiti tecnico-funzionali del servizio

Il servizio di “Compliance normativa” dovrà consentire all'Amministrazione un supporto nell'attuazione degli adempimenti atti ad assicurare la conformità con gli standard, le leggi e i regolamenti in materia di privacy e protezione dei dati (General Data Protection Regulation - Regolamento UE 2016) e della normativa europea e nazionale in ambito cyber (es. NIS 2).

Il Fornitore assume il ruolo e la responsabilità di supportare il DPO dell'Amministrazione e/o soggetti referenti da questa individuati nella definizione, attuazione e monitoraggio della compliance GDPR e NIS2, fornendo analisi, strumenti e implementazioni operative, senza sostituirsi alle responsabilità di presidio e supervisione proprie del DPO. Tale ruolo si esplica, ad esempio, attraverso:

- la predisposizione di analisi di compliance, gap analysis e piani di remediation;
- la produzione di evidenze e deliverable (report, modelli, documentazione GDPR/NIS2);
- il raccordo tra protezione dati e sicurezza cyber;
- il supporto nella gestione del rischio e negli obblighi di compliance normativa.

Il servizio dovrà prevedere, senza oneri aggiuntivi per l'Amministrazione, l'adozione di strumenti e la presenza di competenze specifiche che:

- garantiscano all'Amministrazione l'adozione di un processo per assicurare e mantenere la conformità alla normativa sul lungo periodo;
- consentano l'attuazione degli adempimenti relativi alla privacy;

Il servizio di “Compliance normativa”, in relazione al perimetro IT dell'Amministrazione, dovrà inoltre prevedere:

- il monitoraggio del panorama normativo;
- il supporto all'Amministrazione nella regolamentazione dei processi di protezione dei dati personali;

- la valutazione delle principali fonti di rischio di non conformità cui l'Amministrazione è soggetta;
- l'individuazione delle norme, regole e i principi rilevanti per l'Amministrazione e impatto sulle regole e procedure che dovranno guidare lo svolgimento dell'operatività della stessa. In tale ambito dovrà essere posta l'attenzione ogni volta che viene emessa una nuova normativa, un nuovo regolamento o un nuovo standard al quale attenersi;
- la raccolta e analisi della documentazione disponibile e delle eventuali evidenze/aree di approfondimento;
- la verifica tramite assesment dello stato di attuazione della normativa nell'Amministrazione (AS-IS), con riguardo alle modifiche/cambiamenti richiesti dalla normativa vigente, individuazione dei processi impattati e che potrebbero risultare quindi esposti al rischio di non conformità, valutando anche il grado di rischio di tale esposizione;
- l'identificazione dei requisiti GDPR e della normativa cyber per i diversi macro ambiti (es. governance, processi e metodologie, IT/sicurezza);
- la definizione delle politiche e delle procedure per contrastare efficacemente i rischi individuati;
- l'elaborazione di un piano periodico di verifiche di conformità, al fine di controllare lo stato dell'arte, l'effettiva applicazione degli adeguamenti organizzativi/operativi resisi necessari, il grado di disallineamento e le eventuali carenze nella gestione dei rischi dell'Amministrazione;
- la predisposizione di interventi correttivi, nuovi processi informativi o di formazione;
- l'elaborazione di reportistica periodica e documentazione relativa alle varie attività di compliance;
- il supporto allo sviluppo delle competenze e delle professionalità necessarie a garantire un'efficace applicazione delle regole e dei processi definiti, tramite un adeguato processo di comunicazione e formazione del personale dell'Amministrazione.

In particolare, si indicano a titolo semplificativo e non esaustivo le principali attività nell'ambito del servizio:

- a fronte del registro dei trattamenti dei dati personali, della classificazione dei dati e della valutazione dei rischi:
 - indirizzare gli aspetti IT conseguenti alle politiche di retention dei dati;
 - valutare gli impatti IT nell'attuazione delle policy dei diritti dell'interessato, identificando le azioni di remediation per il superamento dei gap individuati;
- individuare e aggiornare il perimetro dei sistemi IT interessati dal regolamento GDPR;
- predisporre la mappatura tra la classificazione dei dati trattati e le soluzioni tecnologiche da adottare al fine di garantire:
 - un livello minimo di sicurezza per tutti gli applicativi (baseline di sicurezza applicata a tutti i sistemi);
 - l'individuazione e applicazione di misure aggiuntive specifiche in base alla natura e criticità del dato, quali mascheramento, cifratura dei Data base, strong authentication, pseudonymisation;

- identificare i sistemi che raccolgono i consensi al trattamento dati di soggetti esterni ed interni; valutare la compliance rispetto alla normativa; definire e monitorare eventuali piani di rientro;
- garantire l'informativa verso i titolari, i responsabili del trattamento, gli incaricati del trattamento, i soggetti, i partner interni o esterni e le entità sui loro diritti, obblighi e responsabilità in materia di protezione dei dati;
- predisporre modelli per la documentazione tecnica da produrre verso l'Autorità Garante e gli interessati in caso di data breach;
- supportare il monitoraggio del Piano complessivo di interventi IT volti a garantire la compliance al GDPR;
- elaborare di sessioni formative di aggiornamento in tema di GDPR.

Di seguito si indicano, a titolo esemplificativo e non esaustivo, i deliverables documentali prodotti dal servizio:

- report Assessment e Gap Analysis;
- piano degli interventi;
- rapporti di compliance privacy / NIS 2;
- NIS 2 / Perimetro Sicurezza Nazionale Cibernetica Compliance report;
- privacy by design report;
- registro dei trattamenti;
- scheda per il censimento dei trattamenti;
- framework documentale in ambito privacy (es. procedura data breach, metodologia DPIA, nomine a responsabile, informative).

Le risorse impiegate dal Fornitore nella erogazione del servizio dovranno possedere specifiche competenze tecnico-giuridiche e professionali ed essere inserite in programmi di formazione specifica e continua, in base alle evoluzioni del contesto in materia.

Figure professionali

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

- Security Principal;
- Data privacy & protection Specialist;
- Information Security Consultant Senior;
- Information Security Consultant Junior;
- Security Auditor Senior;
- Risk Manager.

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

Metrica di dimensionamento e modalità di remunerazione

Per ciascuna figura professionale è prevista:

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

La metrica di dimensionamento del servizio di “Compliance normativa” è: **giorni/persona**.

La modalità di remunerazione del servizio di “Compliance normativa” è: **a tempo/spesa** oppure **a corpo**.

3.6. Lx.S18 - Vulnerability assessment

Requisiti tecnico-funzionali del servizio

Il servizio di “Vulnerability Assessment” dovrà consentire alle Amministrazioni un esame sistematico di uno o più componenti IT o del sistema informativo per determinare l’adeguatezza delle misure di sicurezza, identificandone le carenze, fornire dati da cui prevedere la loro efficacia e confermare l’adeguatezza di tali misure dopo l’implementazione.

Il servizio deve consentire una verifica dinamica della sicurezza dei dispositivi di rete, del software di base e delle applicazioni dell’Amministrazione allo scopo di identificare eventuali vulnerabilità, configurazioni di sicurezza errate, carenze sui livelli di protezione attivi, applicazioni web e server che esponano il contesto ad attacchi interni ed esterni. Il servizio dovrà essere modulare e configurabile per il singolo host o applicazione.

Gli esiti del servizio consentiranno quindi alle Amministrazioni di elaborare una baseline iniziale (AS-IS) del livello di vulnerabilità e di esposizione del sistema informativo necessaria alla definizione della specifica strategia di sicurezza informatica.

Tale baseline informativa dovrà essere verificata nuovamente nel momento in cui dovessero verificarsi cambiamenti strutturali nell’architettura dei sistemi, della rete o delle applicazioni a seguito, ad esempio:

- Il cambiamento dei sistemi e delle applicazioni del sistema informativo dell’Amministrazione dovuto ad un rinnovamento tecnologico o all’introduzione di vincoli normativi e/o organizzativi;
- l’evoluzione del modello di erogazione dei servizi dell’Amministrazione mediante la reingegnerizzazione dei servizi verso un modello “On-premise”, “Ibrido” o di tipo “Cloud”.

Il servizio dovrà consentire una verifica dinamica della sicurezza dei dispositivi di rete dell’Amministrazione allo scopo di identificare eventuali vulnerabilità, configurazioni di sicurezza errate, carenze sui livelli di protezione attivi che esponano il contesto ad attacchi interni ed esterni.

Per la raccolta di tali informazioni il Fornitore dovrà prevedere strumenti automatizzati senza oneri aggiuntivi per l'Amministrazione. Gli strumenti dovranno essere configurati in modo da non risultare intrusivi (a meno che non sia espressamente concordato con l'Amministrazione).

Il servizio dovrà prevedere almeno le fasi di seguito indicate:

a. Pianificazione.

- definizione dell'ambito di svolgimento del servizio di vulnerability assessment;
- identificazione e condivisione con l'Amministrazione delle metodologie proposte e degli strumenti da adottare e delle modalità di esecuzione;
- raccolta di dati al fine di reperire il maggior numero di informazioni sulla struttura della rete, dei sistemi e delle applicazioni;
- preparazione del piano di test e delle regole di ingaggio.

b. Esecuzione.

- individuazione delle vulnerabilità svolta al fine di collezionare, tramite un set opportuno di strumenti automatizzati e correttamente configurati, una lista delle potenziali vulnerabilità note a cui potrebbero essere soggetti i sistemi analizzati. Tale fase dovrà adattarsi al contesto infrastrutturale specifico ed alle peculiari vulnerabilità associate allo specifico modello di trasporto;
- analisi delle vulnerabilità identificate mediante utilizzo di strumenti di scoring (CVSS). La gravità delle vulnerabilità, del loro impatto potenziale sulla sicurezza e della probabilità che vengano sfruttate da un attaccante vengono stimate;
- esecuzione delle attività secondo un approccio sia di tipo *black box* (senza ausilio di credenziali) che di tipo *grey box* (con ausilio di credenziali);
- network e service discovery, con scansione della rete alla ricerca dei nodi attivi;
- identificazione delle tecnologie adottate e delle relative versioni dei servizi in esecuzione;
- individuazione delle vulnerabilità applicative mediante discovery e testing delle URL, form HTML, componenti Javascript, Ajax, ecc.;
- verifiche atte a valutare la robustezza di infrastrutture Wi-Fi e access point ad uso del personale dipendente dell'Amministrazione e degli utenti esterni;
- individuazione di tecnologie in ambienti non idonei, con conseguente esposizione di rischi;
- verifica della mancanza o non corretta implementazione di tecnologie di prevenzione e riconoscimento di possibili attacchi (sistemi IDS, sistemi IPS, attività di monitoraggio dei log);
- verifica di possibile utilizzo di tecnologie in modi impropri.

c. Prioritizzazione delle vulnerabilità e verifica dei risultati.

- Prioritizzazione delle vulnerabilità individuate secondo policy definite a monte dall'Amministrazione;
- assegnazione delle priorità/severità ai rischi di sicurezza sulla base delle policy concordate con l'Amministrazione;

- correlazione dei risultati delle fasi precedenti e la definizione del piano di rientro (remediation plan);
- produzione di reportistica di sintesi (executive summary) e di dettaglio (technical report) sulle analisi eseguite e rappresentazione delle informazioni qualitative e dimensionali sugli applicativi analizzati, con indicazioni sulle possibili correzioni da apportare.

Il servizio dovrà prevedere, senza oneri aggiuntivi per l'Amministrazione, l'adozione di strumenti e la presenza di risorse professionali con competenze specifiche.

Dal punto di vista tecnico, il servizio dovrà prevedere almeno la compatibilità con i maggiori protocolli di rete di livello application quali FTP/SFTP/FTPS, HTTP/HTTPS, SMTP e di livello network e transport.

Figure professionali

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

- Security Principal;
- Penetration Tester Senior;
- Penetration Tester Junior;
- Information Security Consultant Senior;
- Information Security Consultant Junior;
- Security Solution Architect Senior.

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

Metrica di dimensionamento e modalità di remunerazione

Per ciascuna figura professionale è prevista:

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

La metrica di dimensionamento del servizio di "Vulnerability assessment" è: **giorni/persona**.

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

3.7. Lx.S19 - Penetration testing

Requisiti tecnico-funzionali del servizio

Il servizio di “Penetration testing” dovrà fornire all’Amministrazione un processo operativo di analisi e valutazione dei punti deboli relativi ad una infrastruttura IT.

Il servizio è un test di sicurezza che lancia un attacco informatico simulato per individuare le vulnerabilità in un sistema.

Il risultato del test è un report sulle vulnerabilità che hanno permesso l’accesso non autorizzato al sistema con una stima chiara sulle capacità di difesa e sul livello di penetrazione raggiunto.

A titolo non esaustivo vengono di seguito indicate le categorie di vulnerabilità utilizzabili per il test:

- **vulnerabilità interne al sistema:** che permettono l’accesso sia ad utenti autorizzati che non autorizzati;
- **vulnerabilità esterne al sistema:** relative al modo in cui una organizzazione si connette a Internet e ad altri sistemi esterni. Include server, host, dispositivi e servizi di rete;
- **vulnerabilità delle applicazioni web e mobile:** che derivano da modalità non sicure nella esecuzione di un’applicazione, di un sito web, di un APP.
- **vulnerabilità delle reti wireless:** che permettono l’accesso a dispositivi non autorizzati che fanno parte dell’ambiente protetto dell’organizzazione.
- **vulnerabilità delle API:** relative al funzionamento delle logiche applicative soprattutto per quanto riguarda le meccaniche di autenticazione e autorizzazione.
- **vulnerabilità degli IoT:** relative al funzionamento di tali infrastrutture allo scopo di estrarre informazioni o comprometterne il funzionamento.
- **vulnerabilità connesse agli attacchi di phishing:** relative alla valutazione della suscettibilità degli utenti agli attacchi di “ingegneria sociale”.

Le vulnerabilità possono riguardare sistemi operativi, servizi, configurazioni, server, endpoint, applicazioni Web, reti wireless, dispositivi di rete, dispositivi mobili.

Il servizio di “Penetration Testing” potrà essere svolto dal Fornitore mediante l’adozione di tecnologie e strumenti automatici senza oneri aggiuntivi per l’Amministrazione.

Il Fornitore dovrà svolgere il servizio di “Penetration testing” mediante l’adozione di metodologie e standard di mercato di riferimento quali:

- OWASP Testing Guide;
- OSSTMM;
- Penetration Testing Execution Standard (PTES).

Di seguito vengono indicate le fasi che il servizio di “penetration testing” dovrà prevedere:

- **Information gathering:** raccolta di informazioni sugli asset dell’Amministrazione utili per determinare le potenziali superfici di attacco (es. la scansione delle porte, l’enumerazione di servizi, delle applicazioni, degli utenti, un elenco di e-mail per attacchi di tipo Social Engineering).

- **Exploitation:** stabilire un accesso al sistema, aggirando gli eventuali sistemi di controllo e sicurezza presenti. In questa fase il servizio potrà anche identificare nuove vulnerabilità e codificarne gli exploit.
- **Post Exploitation:** raccolta delle informazioni ottenute (comprese le password) e dei privilegi acquisiti durante la fase di Exploitation.
- **Reporting:** preparazione di report con evidenza delle azioni intraprese all'interno del perimetro definito, delle motivazioni e dei risultati ottenuti.

I Penetration test dovranno poter essere eseguiti nelle seguenti modalità a scelta dell'Amministrazione:

- **White Box:** presuppone conoscenze dettagliate dell'infrastruttura da esaminare, quali documentazione dell'architettura, schemi di rete, codice sorgente delle applicazioni e liste di indirizzi IP presenti nella rete. Mediante le informazioni che vengono fornite è permessa una copertura maggiore ed una panoramica estensiva di ogni possibile vettore di attacco.
- **Black Box:** il test non presuppone precedente conoscenza dell'infrastruttura oggetto di analisi e i tester necessitano di determinare architettura e servizi dei sistemi prima di iniziare l'analisi. L'esaminatore vestirà il ruolo di un attaccante che tenta di compromettere la sicurezza dell'infrastruttura dall'esterno.
- **Grey Box:** il test presuppone conoscenze e informazioni parziali, solitamente si tratta di credenziali per il login. Tale modalità permette di modellare situazioni in cui un hacker, dall'esterno ha ottenuto accesso alla rete interna, oppure per simulare una insider threat. E' una modalità intermedia tra il white box ed il black box, ed è utile a testare in maniera realistica la sicurezza, senza però entrare nel merito di test troppo approfonditi.

Figure professionali

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

- Security Principal;
- Penetration Tester Senior;
- Penetration Tester Junior;
- Forensic Expert.

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

Metrica di dimensionamento e modalità di remunerazione

Per ciascuna figura professionale è prevista:

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)
Capitolato Tecnico Speciale Lotti 3 e 4

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

La metrica di dimensionamento del servizio di “Penetration testing” è: **giorni/persona**.

La modalità di remunerazione del servizio di “Penetration testing” è: **a tempo/spesa** oppure **a corpo**.

3.8. Lx.S20 - Analisi del codice - statico

Requisiti tecnico-funzionali del servizio

Il servizio di “Analisi del codice - statico” dovrà consentire alle Amministrazioni l’identificazione delle vulnerabilità software all’interno del codice (sorgente o binario) delle applicazioni nella fase iniziale del ciclo di vita in modo da poterle eliminare prima della distribuzione.

Questa tipologia di test (anche detta “white box testing”) deve consentire agli sviluppatori di trovare le vulnerabilità di sicurezza nel codice sorgente durante le prime fasi di sviluppo dell’applicazione garantendo la conformità alle linee guida (ad es. owasp) ed agli standard di codifica senza eseguire effettivamente il codice sottostante.

Il termine “applicazione” viene qui inteso come un insieme di righe di codice sorgente elaborate in linguaggi diversi e pagine applicate a contesti di complessità diversa e di differente utilizzo, finalizzate però a rispondere a specifiche esigenze funzionali, ben identificabili nel contesto dell’Amministrazione richiedente.

Più in generale, il perimetro di applicazione del servizio comprende l’analisi statica del codice sorgente delle seguenti categorie: sviluppo custom interno/esterno, open source, software/librerie di terze parti.

L’attività di analisi statica del codice dovrà essere svolta dal Fornitore secondo le best practice internazionali, ed almeno secondo quanto previsto dalle metodologie OWASP TOP 10 e OSSTMM, e dovrà includere almeno i seguenti controlli:

- **Data Validation**: verifica della presenza di vulnerabilità che possono riguardare eventuali dati corrotti in ingresso che possono portare a un comportamento anomalo dell’applicazione;
- **Control Flow**: verifica dei rischi collegati all’assenza di specifiche sequenze di operazioni che, se non eseguite in un certo ordine, potrebbero portare a violazioni sulla memoria o l’uso scorretto di determinati componenti;
- **Semantico**: rilevazione di eventuali problematiche legate all’uso non corretto di determinate funzioni o API (es. funzioni deprecated);
- **Configurazioni**: verifica dei parametri intrinseci di configurazione dell’applicazione;
- **Buffer Validation**: verifica della presenza di buffer overflow exploitabile attraverso la scrittura o lettura di un numero di dati superiore alla reale capacità del buffer stesso.

Si precisa che pur essendo il servizio prevalentemente orientato ad applicazioni in ambiente web, il Fornitore, previo accordo con l'Amministrazione, potrà erogarlo anche su altre tipologie di ambienti, utilizzando il medesimo modello di pricing di seguito definito.

Ove l'Amministrazione fosse dotata di linee guida per lo sviluppo di codice, il servizio potrà essere anche utilizzato a supporto della "compliance" verso tali linee guida.

Il Fornitore nell'ambito del servizio "Testing del codice - statico" dovrà individuare le vulnerabilità critiche come SQL injection, cross-site scripting (XSS), buffer overflow, condizioni di errore non gestite e potenziali back-door.

Di seguito un elenco delle funzionalità base / strumenti a supporto:

- identificazione delle vulnerabilità attraverso l'analisi del codice sorgente e indicazione puntuale delle sezioni di codice relative alle vulnerabilità riscontrate;
- adozione di basi dati di conoscenza quali ad esempio i dati di MITRE ATT&CK utilizzando i dati sempre aggiornati relativi a tattiche, tecniche e mitigazioni delle minacce informatiche;
- verifica dei risultati, individuazione e rimozione dei falsi positivi;
- prioritizzazione delle vulnerabilità individuate e definizione del piano delle azioni correttive (remediation plan);
- produzione di reportistica di sintesi (executive summary) e di dettaglio (technical report) sulle analisi eseguite e rappresentazione delle informazioni qualitative e dimensionali sugli applicativi analizzati, con indicazioni sulle possibili ottimizzazioni da apportare;
- follow up: che consenta di verificare se le azioni correttive adottate sono state efficaci nel mitigare i rischi per la sicurezza informatica individuati.

Dal punto di vista tecnico, nel caso in cui il servizio utilizzi il codice sorgente, dovrà prevedere almeno:

- compatibilità con i principali linguaggi (tra cui .NET, PHP, C#, CC/C++, Java script e TypeScript, HTML, J2EE, ASP, Swift, Python, ABAP) e framework di sviluppo (tra cui React, Angular, Vue.js, Laravel, Spring, Django, Express.js) largamente diffusi.
- Conoscenza degli standard di settore (CVE, CVSS, CWE, ecc.).

Il servizio dovrà prevedere, senza oneri aggiuntivi per l'Amministrazione, l'adozione di strumenti e la presenza di risorse professionali con competenze specifiche.

Nell'esecuzione del servizio il Fornitore dovrà operare in coerenza con le previsioni indicate nelle Linee Guida AgID; in particolare si citano le Linee guida per lo sviluppo del software sicuro nella pubblica amministrazione (allegati tecnici 1, 2, 3 e 4).

Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento del servizio di "Analisi del codice - statico" è: **Numero di applicazioni/anno** secondo le seguenti fasce:

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)
Capitolato Tecnico Speciale Lotti 3 e 4

- Fascia 1: fino a 15 applicazioni;
- Fascia 2: da 16 a 50 applicazioni;
- Fascia 3: oltre 50 applicazioni.

Il significato di “Applicazione”, ove applicabile, può essere ricondotto al Repository di Codice Sorgente (Repository-based): ogni repository Git (o altra VCS) viene considerato un'applicazione singola.

La modalità di remunerazione del servizio “Analisi del codice - statico” 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.

3.9. Lx.S21 - Analisi del codice - dinamico

Requisiti tecnico-funzionali del servizio

Il servizio di “Analisi del codice - dinamico” dovrà consentire alle Amministrazioni l'identificazione delle vulnerabilità all'interno delle applicazioni Web, API Rest e Servizi SOAP in fase di esecuzione e l'analisi dell'esposizione al rischio di attacchi informatici ai sistemi informativi mediante l'utilizzo di tecniche di analisi dinamica.

L'approccio adottato dovrà prevedere il “black box testing” o testing funzionale fondato sull'analisi degli output generati dal sistema o dai suoi componenti in risposta ad input definiti.

L'analisi per l'individuazione delle vulnerabilità dovrà comprendere almeno gli ambiti di seguito riportati.

- **Configurazione:** identificazione delle directory e delle pagine web interessate dal workflow applicativo.
- **Autenticazione:** analisi delle funzionalità di autenticazione per verificare che al loro interno non siano presenti problematiche di sicurezza in particolare:
 - che le credenziali di accesso fornite dagli utenti viaggino attraverso canali di comunicazioni considerati come sicuri;
 - che siano presenti dei meccanismi di enforcing delle credenziali di accesso cioè se il meccanismo di autenticazione e di provisioning dell'applicazione impedisca agli utenti finali l'utilizzo di determinate password classificate comunemente come deboli;
 - che all'interno dell'applicazione siano presenti dei meccanismi di protezione da “attacchi a dizionario”¹. Qualora tali meccanismi siano presenti andrà verificato che non siano aggirabili.
- **Autorizzazione:** verifica della presenza di problematiche di sicurezza legate alla possibilità di elevare i privilegi e i ruoli delle utenze applicative o di accedere a sezioni dell'applicazione protette aggirando i meccanismi di autenticazione e autorizzazione esistenti.

¹ Tecnica di attacco alla sicurezza di un sistema o sottosistema informatico mirata a decifrare un codice o una determinata password utilizzando una lista di parole probabili (detta dizionario).

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)
Capitolato Tecnico Speciale Lotti 3 e 4

- **Validazione dei dati:** verifica della validazione degli input degli utenti al fine di garantire che non siano presenti eventuali criticità di sicurezza.

I controlli effettuati dovranno consentire almeno di:

- verificare i meccanismi di gestione delle sessioni e della loro robustezza;
- verificare se il codice analizzato sia un software dannoso, l'esecuzione dovrà avvenire in particolari ambienti controllati, ove disponibili;
- analizzare il sistema di gestione degli errori dell'applicazione;
- controllare, laddove applicabile, i meccanismi di crittografia;
- verificare i meccanismi di logging e il metodo di gestione delle informazioni;
- verificare le comunicazioni dell'applicativo con soggetti esterni come client, DB, LDAP;
- integrazione nelle pipeline DevOps e CI/CD;
- verificare i web service, applicazioni Legacy ed altre API esterne;
- supportare l'adozione di basi dati di conoscenza quali ad esempio MITRE ATT&CK utilizzando i dati sempre aggiornati relativi a tattiche, tecniche e mitigazioni delle minacce informatiche.
- Conoscenza degli standard di settore (CVE, CVSS, CWE, ecc.);

I risultati delle analisi del codice dovranno permettere di mitigare i seguenti principali rischi, tra cui si riportano a titolo esemplificativo e non esaustivo:

- *Injection*
- *Broken Authentication*
- *Sensitive Data Exposure*
- *XML External Entities (XXE)*
- *Broken Access Control*
- *Security Misconfiguration*
- *Cross-Site Scripting (XSS)*
- *Insecure Deserialization*
- *Using Components with Known Vulnerabilities*
- *Insufficient Logging e Monitoring*

Dovranno inoltre essere identificate e rilevate le principali tipologie di vulnerabilità potenziali, tra cui si riportano a titolo esemplificativo e non esaustivo:

- *Cross-Site Scripting;*
- *Format String;*
- *Integer Overflows;*
- *Null Byte Injection;*
- *Path Traversal;*
- *Remote File Inclusion;*
- *SSI Injection;*

- *SQL Injection;*
- *XPath Injection;*
- *XML Injection;*
- *XQuery Injection.*

Ove l'Amministrazione fosse dotata di linee guida per lo sviluppo di codice, il servizio potrà essere anche utilizzato a supporto della "compliance" verso tali linee guida.

Il servizio dovrà essere svolto secondo le best practice internazionali, e almeno secondo quanto previsto dalle metodologie OWASP TOP 10 e OSSTMM.

Il Fornitore dovrà garantire la disponibilità delle seguenti funzionalità base / strumenti a supporto:

- identificazione delle vulnerabilità attraverso l'esecuzione di scansioni;
- verifica dei risultati, individuazione e rimozione dei falsi positivi;
- assegnazione automatica delle priorità/severità ai rischi di sicurezza sulla base delle policy concordate con l'Amministrazione;
- correlazione dei risultati delle fasi precedenti con la definizione del piano di rientro (remediation plan);
- produzione di reportistica di sintesi (executive summary) e di dettaglio (technical report) sulle analisi eseguite e rappresentazione delle informazioni qualitative e dimensionali sugli applicativi analizzati, con indicazioni sulle possibili correzioni da apportare.

Dal punto di vista tecnico, il servizio dovrà prevedere almeno la compatibilità con i principali linguaggi (tra cui .NET, PHP, C#, CC/C++, Java script e TypeScript, HTML, J2EE, ASP, Swift, Python, ABAP) e framework di sviluppo (tra cui React, Angular, Vue.js, Laravel, Spring, Django, Express.js) largamente diffusi.

Il servizio dovrà prevedere, senza oneri aggiuntivi per l'Amministrazione, l'adozione di strumenti e la presenza di risorse professionali con competenze specifiche.

Nell'esecuzione del servizio il Fornitore dovrà operare in coerenza con le previsioni indicate nelle Linee Guida AgID; in particolare si citano le Linee guida per lo sviluppo del software sicuro nella pubblica amministrazione (allegati tecnici 1, 2, 3 e 4).

Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento del servizio di "Analisi del codice - dinamico" è: **numero di applicazioni/anno**, secondo le seguenti fasce:

- Fascia 1: fino a 15 applicazioni;
- Fascia 2: da 16 a 50 applicazioni;
- Fascia 3: oltre 50 applicazioni.

Il significato di “Applicazione”, ove applicabile, può essere ricondotto alla URL o Endpoint Principale (Applicazione Web): Un'applicazione è definita come un insieme di pagine web e funzionalità raggiungibili tramite un dominio/sottodominio univoco.

La modalità di remunerazione del servizio “Analisi del codice - dinamico” 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.

3.10. Lx.S22 - Analisi del codice - mobile

Requisiti tecnico-funzionali del servizio

Il servizio di “Analisi del codice - mobile” deve eseguire test mirati sulle applicazioni di tipo mobile consentendo la rilevazione delle vulnerabilità di sicurezza.

Si noti che l’ambito del servizio dovrà includere non solo l’analisi del codice e l’esecuzione dell’applicazione ma dovrà anche riguardare tutte le interfacce verso altri sistemi e/o applicazioni così come altre risorse collegate che potrebbero avere un impatto sulla sicurezza globale del sistema.

Ove l’Amministrazione fosse dotata di linee guida per lo sviluppo di codice, il servizio potrà essere anche utilizzato a supporto della “compliance” verso tali linee guida.

Il servizio dovrà essere svolto secondo le best practice internazionali, e almeno secondo quanto previsto dalle metodologie OWASP TOP 10 e MASTG (Mobile Application Security Testing Guide). Il Fornitore, nell’ambito del servizio “Analisi del codice - mobile” dovrà garantire la disponibilità per l’Amministrazione almeno delle seguenti funzionalità base:

- individuazione delle vulnerabilità mediante tecnica di analisi statica e dinamica;
- verifica dei risultati, individuazione e rimozione dei falsi positivi;
- assegnazione automatica delle priorità/severità ai rischi di sicurezza sulla base delle policy concordate con l’Amministrazione;
- correlazione dei risultati delle fasi precedenti e definizione del piano di rientro (remediation plan);
- produzione di reportistica di sintesi (executive summary) e di dettaglio (technical report) sulle analisi eseguite e indicazione delle possibili correzioni da apportare; in conformità agli standard più comuni OWASP Mobile Top 10, OWASP MASVS (Mobile Application Security Verification Standard), ADA MASA, FFIEC, PCI, NIAP, HIPAA, GDPR, CWE.
- adozione di basi dati di conoscenza quali ad esempio i dati di MITRE ATT&CK utilizzando i dati sempre aggiornati relativi a tattiche, tecniche e mitigazioni delle minacce informatiche.
- analisi e gestione delle policy di accesso ai dati e alle funzioni del dispositivo;
- assegnazione alle vulnerabilità di un punteggio numerico secondo lo standard CVSS.

Il servizio dovrà prevedere, senza oneri aggiuntivi per l’Amministrazione, l’adozione di strumenti e la presenza di risorse professionali con competenze specifiche.

Dal punto di vista tecnico, il servizio dovrà prevedere la compatibilità con almeno i seguenti principali sistemi operativi: Android e iOS.

Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento del servizio di “Analisi del codice - mobile” è: **numero di applicazioni/anno** secondo le seguenti fasce:

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l’affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)
Capitolato Tecnico Speciale Lotti 3 e 4

- Fascia 1: fino a 15 applicazioni;
- Fascia 2: da 16 a 50 applicazioni;
- Fascia 3: oltre 50 applicazioni.

Il significato di “Applicazione”, ove applicabile, può essere ricondotto al Pacchetto Identificabile (Binary): Ogni file binario o pacchetto di installazione univoco scaricato dallo store o inviato per il test, indipendentemente dalla versione.

La modalità di remunerazione del servizio “Analisi del codice - mobile” è: **canone annuale**
L'ordine di acquisto del servizio dovrà avere una durata minima di 12 (dodici) mesi.

3.11. Lx.S23 – Controllo terze parti (supply-chain di approvvigionamento)

Requisiti tecnico-funzionali del servizio

Il servizio di “Controllo terze parti (supply-chain di approvvigionamento)” dovrà fornire alle Amministrazioni un supporto nella gestione degli aspetti di sicurezza della “supply chain” identificando, analizzando e riducendo al minimo i rischi associati al lavoro con le organizzazioni esterne come parte della supply chain.

Per supply chain (“catena di fornitura”) si intende una rete di organizzazioni con un insieme collegato di risorse e processi coinvolti nelle attività di produzione o di erogazione di servizi fino al cliente o utente finale.

I possibili scenari di rischio legati alle tecnologie dell'informazione e comunicazione (ICT) all'interno della catena di fornitura sono dipendenti dalla tipologia di prodotto o servizio o dal settore specifico in cui opera la PA possono essere:

- rischio di sicurezza dei dati: furto o compromissioni di dati critici, modifica e corruzione dei dati gestiti o acceduti da fornitori causati dall'applicazione di misure di sicurezza inadeguate da parte dei fornitori stessi;
- **vulnerabilità del software**: software, sia di base che applicativo, sia open source che proprietario, che presenta vulnerabilità o comunque di qualità insufficiente, compromissione della distribuzione del software e difficoltà di aggiornamento;
- **presenza di malware all'interno del software fornito da terze parti**: inserimento di software malevolo in fase di sviluppo, di distribuzione o in esercizio;
- **vendor lock-in**: dipendenza da un unico fornitore per servizi essenziali;
- **Indisponibilità di dati e servizi**: cessazione di attività da parte del fornitore, incidenti a sistemi, software, TLC, carenza di personale.

Il servizio basato su un approccio metodologico di Risk Management, sia quantitativo sia qualitativo delle terze parti, dovrà prevedere senza oneri aggiuntivi per l'Amministrazione l'adozione di strumenti e la presenza di competenze specifiche che consentano:

- la raccolta e studio delle informazioni relative ai processi di gestione AS-IS dei fornitori da parte dell'amministrazione e della normativa vigente applicabile (es: NIS, NIS 2, Perimetro cibernetico) e le implicazioni con il codice degli appalti;
- l'individuazione e definizione dei requisiti di sicurezza delle informazioni con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, o trasmettere informazioni dell'Amministrazione, o fornire componenti dell'infrastruttura IT per il trattamento di tali informazioni;
- il censimento e analisi delle terze parti sulla base di categorie di servizio e classificazione dei fornitori sulla base del servizio erogato;
- la revisione degli accordi con i fornitori al fine di allineare i requisiti correlati ai rischi di sicurezza alla sicurezza delle informazioni associati a servizi e prodotti della filiera di fornitura per l'ICT;
- la gestione degli aspetti legali delle responsabilità in materia di sicurezza delle informazioni e delle relazioni con le terze parti;
- il monitoraggio regolare, riesame periodico e audit dei servizi erogati da parte dei fornitori rispetto a requisiti e obblighi di conformità;
- il supporto al change management nei processi di gestione delle forniture;
- il supporto all'adozione strumenti di QA e security testing per la validazione dei deliverable e implementazione di Security Gate nell'ambito del ciclo di vita dei sistemi informativi;
- la definizione di nuovi approcci per la gestione della catena di approvvigionamento anche mediante l'ausilio di strumenti informatici e in linea con il principio della digitalizzazione;
- monitoraggio dei piani di remediation della catena di approvvigionamento;
- esecuzione di assessment/audit sulla base alle caratteristiche del servizio individuato in termini di processi e relativi controlli che la terza parte e i suoi subappaltatori hanno messo in atto per mitigare i rischi relativi al servizio.

Di seguito un elenco esemplificativo e non esaustivo dei possibili prodotti di fornitura oggetto del servizio:

- procedura/ documento con identificazione ruoli e responsabilità;
- documento che censisce e categorizza i fornitori rispetto ai servizi esternalizzati;
- prioritizzazione dei fornitori rispetto in considerazione della criticità del servizio esternalizzato e dei dati trattati;
- checklist per la conduzione di audit/verifiche sulle misure di sicurezza tecniche/organizzative di matrice cyber e data protection a seconda della categoria di appartenenza del fornitore;
- report sulle verifiche/audit condotti sui fornitori considerati prioritari.

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)
Capitolato Tecnico Speciale Lotti 3 e 4

Figure professionali

Per erogare il presente servizio il Fornitore dovrà disporre dei seguenti i profili professionali (per il dettaglio dei profili si rimanda all'appendice Profili Professionali):

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

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

Metrica di dimensionamento e modalità di remunerazione

Per ciascuna figura professionale è prevista:

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

La metrica di dimensionamento del servizio di "Controllo terze parti (supply-chain di approvvigionamento)" è: **giorni/persona**.

La modalità di remunerazione del servizio di "Controllo terze parti (supply-chain di approvvigionamento)" è: **a tempo/spesa** oppure **a corpo**.

3.12. Modalità di erogazione in configurazione ibrida o on-premise

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

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

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

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

4. REQUISITI DI ESECUZIONE

4.1. ISO 9001

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

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

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

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

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

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

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

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

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

4.2. ISO 27001

Ai fini dell'esecuzione dell'Accordo Quadro, il Fornitore dovrà essere in possesso di una valutazione di conformità del sistema di gestione alla norma UNI EN ISO 27001, idonea, pertinente e proporzionata al seguente ambito di attività: **servizi di consulenza tecnico-specialistica, organizzativa, strategica nell'ambito della sicurezza informatica e/o della continuità operativa.**

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

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

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

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

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

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

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

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

4.3. DNSH

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

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

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

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

- a) il fornitore potrà, proporre, senza oneri aggiuntivi per la PA, l'utilizzo di centri dati e sale server diversi, ma comunque con funzionalità equivalenti o superiori rispetto a quelle eventualmente indicate in offerta tecnica e comunque in possesso dei requisiti richiesti nel presente documento. Qualora la sostituzione sia proposta in corso di esecuzione contrattuale, trova applicazione quanto previsto al paragrafo 12.4 del Capitolato Tecnico Generale;

- b) qualora non risulti percorribile l'opzione di cui al precedente punto, potrà trovare applicazione apposita condizione risolutiva, come meglio indicato nell'Accordo Quadro;

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

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

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

5. FASI OPERATIVE DELLA FORNITURA

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

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

Di seguito le fasi operative della fornitura:

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

5.1. Presa in carico e startup

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

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

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

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

Si precisa che almeno il 50% delle risorse professionali impiegate dal Fornitore nelle attività di presa in carico e startup e dei referenti tecnici delle attività dovranno successivamente essere impiegati nell'erogazione dei servizi.

La fase di presa in carico e startup dovrà essere completata entro il termine massimo di 30 giorni solari dalla data di approvazione del Piano da parte dell'Amministrazione, salvo diverso termine concordato con l'Amministrazione.

5.2. Modalità di attivazione dei servizi

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

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

- gli interventi dovranno essere effettuati in fasce orarie definite dall'Amministrazione, coerentemente con le proprie esigenze di operatività;

- l'operatività del servizio dovrà essere garantita anche durante la fase intermedia di test e collaudo;
- l'impatto delle operazioni di roll-out e installazione sulla normale operatività delle sedi dovrà essere ridotto all'essenziale.

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

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

Nel caso in cui 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.

5.3. Fine fornitura

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

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

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

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

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

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

Sono incluse nelle attività di trasferimento:

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

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

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

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

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

5.4. Exit Strategy e Grace Period

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

Al termine della durata contrattuale di ogni singolo Contratto esecutivo, per un periodo pari a 30 giorni, altrimenti detto grace period, il Fornitore si obbliga, senza oneri aggiuntivi, a mettere a disposizione della PA i dati di quest'ultima, ai fini del relativo recupero. Il Fornitore si obbliga a dare idonee garanzie dell'eliminazione e/o avvenuta inaccessibilità dei dati della PA. In ogni caso, il Fornitore si impegna a dare supporto alla PA per il grace period, senza oneri aggiuntivi (Exit strategy).

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

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

6. MODALITÀ DI EROGAZIONE

6.1. Risorse da impiegare nell'affidamento dei servizi

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

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

Per l'accettazione del personale proposto, l'Amministrazione si riserva la possibilità di procedere ad un colloquio tecnico di approfondimento per verificare la corrispondenza delle competenze ed expertise riportate nel CV e l'effettivo possesso. In tal caso il Fornitore dovrà rendere disponibile al colloquio la risorsa entro 3 giorni lavorativi dalla richiesta.

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

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

Vincoli temporali			
Attività	Evento	Giorni	Note
Consegna all'Amministrazione dei CV delle risorse PRESA IN CARICO E STARTUP e dei responsabili tecnici	Stipula del Contratto esecutivo	5 giorni lavorativi	Allegato al piano di PRESA IN CARICO E STARTUP
Consegna all'Amministrazione dei CV delle risorse professionali e dei ruoli di interfaccia con l'Amministrazione	Stipula del Contratto esecutivo	10 giorni lavorativi	Allegato al piano di lavoro generale
Colloquio	Richiesta di colloquio	3 giorni lavorativi	
Disponibilità della risorsa nei team di lavoro	Comunicazione dell'esito positivo del colloquio	3 giorni lavorativi	In funzione degli specifici piani approvati
Consegna all'Amministrazione 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

Tabella 2 – Vincoli temporali

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

6.2. Competenze richieste

Il Fornitore dovrà mettere in campo per l'erogazione dei servizi oggetto di fornitura tutte le competenze di natura tecnica, funzionale, metodologica e organizzativa, tali da affrontare le

eventuali problematiche e proporre, realizzare e gestire le relative soluzioni, nei contesti specifici dell'Amministrazione.

Le competenze che il Fornitore mette a disposizione devono essere descritte, dimostrate, possedute e messe a disposizione a livello di Raggruppamento di Imprese o Consorzio, in termini di strutture organizzative, metodologie, centri di competenza, risorse professionali, esperienze pregresse.

Nell'Appendice 2 al Capitolato Tecnico Speciale "Profili Professionali" sono indicate le competenze, le conoscenze e le relative certificazioni/credenziali delle risorse professionali che dovranno essere impiegate dal Fornitore per l'esecuzione dei servizi.

6.3. Comunicazioni e Approvazioni

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

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

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

6.4. Modalità di Approvazione

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

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

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

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

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

Per i servizi oggetto di fornitura, nel caso si verificano situazioni “anomale” che, a giudizio della Amministrazione, sia per numerosità, sia per gravità non consentano lo svolgimento o la prosecuzione delle attività, l'Amministrazione procederà alla sospensione delle verifiche di conformità del servizio, la cui riattivazione dovrà avvenire entro il nuovo termine fissato dalla stessa Amministrazione.

6.5. Verifiche di conformità

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

6.6. Azioni contrattuali

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

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

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

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

Rilievi

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

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

I rilievi possono essere emessi dal Direttore dell'esecuzione della Amministrazione, dai responsabili di progetto e/o di servizio della Amministrazione e/o da strutture della Amministrazione preposte o di

supporto al controllo e/o monitoraggio della fornitura e sono formalizzati attraverso una nota di rilievo, ognuna delle quali potrà contenere uno o più rilievi.

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

Penali

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

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

6.7. Monitoraggio

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

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

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

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

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

Reportistica e strumenti di monitoraggio

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

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

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

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

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

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

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

6.8. Dimensionamento dei servizi

A canone

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

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

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

A corpo

La modalità a corpo è utilizzata per attività di tipo progettuale. Nella modalità a corpo la responsabilità del risultato è affidata al fornitore, il quale organizza le proprie risorse professionali, tecniche e metodologiche per soddisfare le richieste.

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

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

proprie spese per rilasciare un prodotto conforme funzionalmente e tecnicamente ai requisiti approvati.

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

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

Tabella 3 - Milestone

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

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

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

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)
Capitolato Tecnico Speciale Lotti 3 e 4

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

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

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

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

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

A consumo

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

6.9. Pianificazione e Consuntivazione

Piano della Qualità Generale dell'Accordo quadro

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

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

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

Piano della Qualità Specifico di Contratto esecutivo

Per ciascun Contratto esecutivo il fornitore dovrà produrre un Piano della Qualità personalizzato sull'ambiente funzionale e tecnologico 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 ai servizi e sia le eventuali deroghe da quanto previsto nel Piano della Qualità Generale. Nel caso in cui per un determinato capitolo non ci siano differenze rispetto al Piano di Qualità Generale dell'AQ occorre solo riportare il riferimento al suddetto piano.

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

Piani di Lavoro

Il Fornitore dovrà predisporre, con le tempistiche indicate nel Capitolato Tecnico Generale, e mantenere costantemente aggiornato il Piano di lavoro generale comprensivo di:

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

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

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

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

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

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 a corpo/a consumo, 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.

Consuntivazione

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

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

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

6.10. Orario di erogazione dei servizi

Di seguito gli orari di servizio della fornitura.

Ambito dei Servizi	Orario
Servizi progettuali a corpo/a consumo dimensionati in giorno persona	Orario base: lunedì – sabato: 08:00 – 20:00 Orario avanzato: lunedì – sabato 20:00 – 08:00, domeniche e festivi

- Servizio Formazione e security Assessment - Servizi a canone	Orario standard: lunedì – sabato: 08:00 – 20:00
- Piattaforme e strumenti a supporto della erogazione dei servizi	H24, 7 gg su 7, 365 gg anno

Tabella 4 – Orari di servizio

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

Si precisa che:

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

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

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

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

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

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

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

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

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