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

APPENDICE 3 - CONTESTO TECNICO LOTTO 2

INDICE DEL DOCUMENTO

1 PREMESSA

La presente Appendice è parte integrante della documentazione di gara e definisce le caratteristiche e i requisiti per l'affidamento dei servizi di Compliance e controllo in ambito Sicurezza informatica per le Pubbliche Amministrazioni.

Le prescrizioni contenute nel presente documento, 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 documento le seguenti Appendici:

Appendice 3A – Indicatori di Qualità - Lotto 2

Appendice 3B – Profili Professionali - Lotto 2

2 OGGETTO

Relativamente al **Lotto 2**, l'oggetto della fornitura comprende i seguenti servizi:

ID Servizio	Servizio
L2.S16	Security Strategy
L2.S17	Vulnerability Assessment
L2.S18	Testing del codice – Statico
L2.S19	Testing del codice – Dinamico
L2.S20	Testing del codice – Mobile
L2.S21	Supporto all'analisi e gestione degli incidenti
L2.S22	Penetration Testing
L2.S23	Compliance normativa

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

- L2; è l'identificativo del numero del Lotto;
- S*n;* ove *n* è il numero progressivo del Servizio.

3 DESCRIZIONE DEI SERVIZI

I servizi di Compliance e controllo hanno l'obiettivo di mettere a disposizione dell'Amministrazione risorse e strumenti finalizzati alla realizzazione del "progetto di sicurezza" ovvero all'insieme di misure da adottare finalizzate alla identificazione dello stato di sicurezza del sistema informativo e alla sua protezione. Il "progetto di sicurezza" dovrà pertanto consentire all'Amministrazione di:

- identificare il livello iniziale di vulnerabilità e di robustezza delle componenti infrastrutturali ed applicative del proprio sistema informativo;
- definire una strategia di governance della sicurezza informatica inerenti gli aspetti tecnologici, organizzativi e normativi;
- identificare le esigenze in termini di fabbisogni di beni/servizi di sicurezza di cui l'Amministrazione dovrà approvviggionarsi per attuare le misure di difesa ed in particolare relativamente ai servizi del Lotto 1;
- esercitare una azione di controllo imparziale sulla corretta esecuzione dei servizi di sicurezza del Lotto 1 e sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

In particolare l'azione di controllo imparziale sulla esecuzione dei servizi del Lotto 1 rende necessario differenziare il ruolo che assumono i fornitori di ciascuno dei due Lotti. In particolare, il fornitore del Lotto 1 è impegnato ad erogare i servizi "core" di sicurezza volti appunto alla tutela della sicurezza dei perimetri tecnologici delle infrastrutture nonché alla protezione delle informazioni della PA, mentre il fornitore del Lotto 2 è colui che eroga servizi di "verifica" volti alla misura dello stato di salute della sicurezza dei sistemi informativi e di supporto della PA nella identificazione dei «fabbisogni» in ambito servizi e forniture di sicurezza ICT.
Mediante l'utilizzo dei servizi oggetto di fornitura del Lotto 2, il fornitore dovrà quindi supportare l'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.

Relativamente alle attività di analisi del rischio AgID, nel suo ruolo di definizione di programmi di sicurezza preventiva a supporto delle amministrazioni, ha messo a disposizione un tool di valutazione e trattamento del rischio cyber.
Questo strumento, già in uso presso un elevato numero di amministrazioni, consente ad ogni PA di effettuare le operazioni di self assessment, predisporre gli opportuni piani di trattamento ed eseguire il monitoraggio delle iniziative volte a ridurre il livello di rischio informatico.

Il Fornitore sarà chiamato ad erogare i servizi in funzione delle esigenze dell'Amministrazione, e assicurando la disponibilità di risorse, strumenti, 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 ed organizzativo dell'Amministrazione contraente, nonché delle sue specificità funzionali 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 sicurezza informatica.

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 adeguata 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 documento.

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

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

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

La modalità di esecuzione dei servizi di "Compliance e controllo" è di tipo **"on-site"**: ovvero primariamente presso le sedi dall'Amministrazione, ove dalla stessa indicate; in alternativa presso la sede del Fornitore**.**

3.1 L2.S16 - Security Strategy

3.1.1 Requisiti tecnico-funzionali del servizio

Il servizio di Security Strategy dovrà fornire all'Amministrazione un supporto volto a individuare le linee strategiche in materia di sicurezza ICT, di definire e monitorare le relative azioni strategiche adottate, al fine di realizzare un "progetto di sicurezza" unitario e coerente.

Di seguito sono proposti gli ambiti di intervento del servizio di Security Strategy.

- **Supporto dell''Amministrazione nella definizione e controllo delle scelte strategiche inerenti il governo della Sicurezza delle informazioni, degli indirizzi organizzativi, tecnologici e dell'approccio da adottare a fronte di nuovi paradigmi architetturali, 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 del "progetto di sicurezza" informatica dell'Amministrazione che tenga in considerazione almeno i seguenti aspetti, quali:

- “Governance” degli asset e dei processi
- “Management” ovvero corretta modalità di gestione della sicurezza (network, application, content, data center, identity)
- “Awareness” degli utenti verso i rischi di sicurezza
- “Incident” processi, soluzioni e servizi di controllo delle infrastruttutre critiche
- “Compliance” normativa

- verifica costante di allineamento del “progetto di sicurezza” dell’Amministrazione con le linee guida, le direttive e normative a livello nazionale ed europeo;
- 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 modello IT della sicurezza (on- premise, cloud, ibrido) dell’Amministrazione;
- supporto dell’Amministrazione nel processo di trasformazione digitale, di trasformazione della tecnologia dell’IT e della sicurezza dell’Amministrazione per adattarsi al Cloud e per affrontare ambienti di minaccia sempre pià sofisticati;
- 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;
- partecipazione a gruppi di lavoro, comitati, tavoli di coordinamento, per la definizione delle strategie, l’analisi delle esigenze e la produzione di documentazione;
- monitoraggio della conduzione e reporting dei risultati dell’attività.

- **Supporto dell''Amministrazione nella definizione delle scelte strategiche inerenti l'identificazione dei fabbisogni di beni e servizi in materia di IT 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:

- predisposizone di studi e analisi di mercato volte alla identificazione 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 strategiche 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 alle Amministrazioni nella fase di analisi e valutazione delle stime quantitative ed economiche relative a servizi di sicurezza oggetto di acquisizione del Lotto 1 ed in particolare per i servizi con modalità di remunerazione "a corpo".
- 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.

Il Fornitore, ove richiesto, dovrà supportare l'Amministrazione nella predisposizione e stesura del Piano di Fabbisogni e nella verifica tecnico-economica del Piano Operativo presentato dal Fornitore dei Lotti dei servizi di sicurezza "da remoto" o di altra inizitiva a cui l'Amministrazione intende aderire.

Nel caso specifico dei servizi di sicurezza da remoto (Lotto 1 della presente iniziativa), il Fornitore dovrà quindi 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. Egli dovrà inoltre provvedere alla verifica della completezza del documento di Contesto Tecnologico ed Applicativo, parte integrante del Piano stesso.

Nella successiva fase, il Fornitore dovrà 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.

Il Fornitore dovrà supportare l'Amministrazione anche nell'elaborazione della richiesta di eventuali modifiche e/o integrazioni da apportare al documento e/o di aggiornamenti del Piano dei fabbisogni e del Piano Operativo, reiterando, laddove necessario, il medesimo processo sopra descritto.

3.1.2 Team di lavoro

Per erogare il presente servizio il fornitore dovrà disporre delle competenze, esperienze e capacità richieste ai profili professionali indicati nel seguito, che devono, tutte, **obbligatoriamente** fare parte del Team di Lavoro (o Team Ottimale) del servizio.
Il Team di Lavoro è sotto la responsabilità e l'organizzazione del fornitore.
Profili Professionali previsti nel Team di Servizio Security Strategy (per il dettaglio dei profili si rimanda all'Appendice 3B Profili Professionali)

- Security Principal

- Security Solution Architect
- Senior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

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

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

3.1.3 Metrica e modalità di remunerazione

La metrica del servizio di "Security Strategy" è:

- **giorni/persona del team ottimale**

La modalità di remunerazione del servizio di "Security Strategy" è:

- **progettuale (a corpo)**

3.2 L2.S17 - Vulnerability assessement

3.2.1 Requisiti tecnico-funzionali del servizio

Il servizio di "Vulnerability Assessment" dovrà consentire alle Amministrazione di identificare lo stato di esposizione alle vulnerabilità mediante la raccolta di informazioni concernente i servizi erogati, le applicazioni, l'architettura e le componenti tecnologiche.

Il servizio è indirizzato principalmente alle Amministrazione che, in fase di definizione della strategia di sicurezza, necessitano di delineare un iniziale valutazione dello stato di sicurezza del sistema informativo e dello stato di esposizione alle vulnerabilità.

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 serventi che espongano 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 di:

- una evoluzione dei sistemi e delle applicazioni del sistema informativo dell'Amministrazione dovuto ad un rinnovamento tecnologico o all'introduzione di vincoli normativi e/o organizzativi;
- una evoluzione del modello di erogazione dei servizi dell'Amministrazione mediante la migrazione dei sistemi e delle applicazioni 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 espongano il contesto ad attacchi interni ed esterni.

Per la raccolta di tali informazioni il Fornitore potrà avvalersi di strumenti automatizzati senza oneri aggiuintivi per l'Amministrazione al fine di rilevare le potenziali vulnerabilità. 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 sotto elencate.

a. **Pianificazione.**

   - definizione dell'ambito di svolgimento del servizio di vulnerability assessement;
   - identificazione e condivisione con l'Amministrazione delle metodologie proposte e degli strumenti da adottare e delle modalità di esecuzione;
   - raccolta di informazioni svolta 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;
- 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 anche la robustezza di infrastrutture Wi-Fi e access point ad uso del personale dipendente dell'Amministrazione e del personale esterno;
- individuazione di tecnologie in ambienti non idonei, con conseguente esposizione di rischi;
- mancanza o non corretta implementazione di tecnologie di prevenzione e riconoscimento di possibili attacchi (sistemi IDS, sistemi IPS, attività di monitoraggio dei log);
- utilizzo di tecnologie in modi impropri.

c. **Prioritizzazione delle vulnerabilità e verifica dei risultati.**

- Le vulnerabilità individuate dovranno essere prioritizzate 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 ottimizzazioni 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:

- compatibilità con i maggiori protocolli di rete di livello application quali FTP/SFTP/FTPS, HTTP/HTTPS, SMTP e di livello network e transport.

3.2.2 Team di lavoro

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

Profili Professionali previsti nel Team di Servizio Vulnerability Assessment (per il dettaglio dei profili si rimanda all'Appendice 3B Profili Professionali)

- Security Principal
- Senior Penetration tester
- Junior Penetration tester

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

3.2.3 Metrica e modalità di remunerazione

La metrica del servizio di "Vulnerability Assessement" è:

- **giorni/persona del team ottimale**

La modalità di remunerazione del servizio di "Vulnerability Assessement" è:

- **progettuale (a corpo)**

3.3 L2.S18 - Testing del codice - statico

3.3.1 Requisiti tecnico-funzionali del servizio

Il servizio di "Testing 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.

ll termine applicazione viene qui inteso come un insieme di righe di codice elaborate in linguaggi diversi ed 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.

Il Fornitore nell'Offerta Tecnica dovrà specificare il tipo di supporto che sarà richiesto all'Amministrazione per l'erogazione del servizio, con esplicita indicazione delle singole attività per cui si richiede supporto ed effort stimato, con particolare riferimento alle tempistiche e alle modalità di consegna del codice oggetto di analisi.

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 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 pericoloso di determinate funzioni o API (es. funzioni deprecate);
- 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.

Il Fornitore nell'ambito del servizio "Testing del codice - statico" dovrà individuare le vulnerabiltà 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;
- 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.

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

- compatibilità con i principali linguaggi e framework di sviluppo largamente diffusi (tra cui almeno .NET, PHP, C/C++, Java, J2EE, ASP, Swift, Python);

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).

3.3.2 Metrica e modalità di remunerazione

La metrica del servizio di "Testing del codice - statico" è:

- **Numero di applicazioni**

La modalità di remunerazione del servizio "static application security testing" è:

- **singola esecuzione,** nel caso in cui il servizio sia erogato per unica scansione (*one time*);

- **Numero di applicazioni/anno**

secondo le seguenti fasce:

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

La modalità di remunerazione del servizio "static application security testing" è:

- **canone annuale**, nel caso in cui il servizio sia erogato in modalità continua (*scansioni periodiche*).

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

3.4 L2.S19 - Testing del codice - dinamico

3.4.1 Requisiti tecnico-funzionali del servizio

Il servizio di "Testing del codice - dinamico" dovrà consentire alle Amministrazioni l'identificazione delle vulnerabilità all'interno delle applicazioni Web 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.
- **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;
- verficare 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;

[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).

- verificare le comunicazioni dell'applicativo con soggetti esterni come client, DB, LDAP, web service, applicazioni Legacy ed altre API esterne.

Il servizio dovrà agire mitigando 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 !njection;*
- *Path Traversal;*
- *Remote File !nclusion;*
- *SS! !njection;*
- *SQL !njection;*
- *XPath !njection;*
- *XML !njection;*
- *XQuery !njection*

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

Il servizio prevede tre diversi profili di erogazione, a seconda della tipologia di applicazione oggetto di analisi, come specificato nella seguente tabella:

Profilo	Tipologia applicazione
Bronze	Applicazioni non critiche che consentono la visualizzazione di pagine di contenuto informativo (siti web statici)
Silver	Applicazioni costituite da più form (siti web dinamici) e con funzionalità di autenticazione
Gold	Applicazioni critiche con funzionalità complesse e di tipo transazionale (ad esempio pagamenti)

Il Fornitore, nell'ambito del servizio "Testing del codice - dinamico" dovrà garantire per tutti i profili di erogazione sopra citati, la disponibilità per l'Amministrazione almeno 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 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 ottimizzazioni da apportare.

Inoltre, per i profili Silver e Gold sono previste le seguenti funzionalità aggiuntive:

Funzionalità	Profilo Silver	Profilo Gold
Definizione di scansioni personalizzate	**X**	**X**
Esecuzione di test di autenticazione multilivello	**X**	**X**
PCI Compliance	**X**	**X**
Esecuzione di test manuali sulle applicazioni in fase di esecuzione	**X**	**X**
Creazione personalizzata di *business logic test*		**X**
Proof of concept delle vulnerabilità riscontrate		**X**

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

- compatibilità con i principali linguaggi e framework di sviluppo largamente diffusi (tra cui almeno .NET, PHP, C/C++, Java, J2EE, ASP, Swift, Python).

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).

3.4.2 Metrica e modalità di remunerazione

La metrica del servizio di "Testing del codice - dinamico" è:

- **numero di Applicazioni per profilo (Bronze, Silver e Gold)/anno**

secondo le seguenti fasce:

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

La modalità di remunerazione del servizio "Testing 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.

3.5 L2.S20 - Testing del codice - mobile

3.5.1 Requisiti tecnico-funzionali del servizio

Il servizio di "Testing del codice - mobile" deve consentire alle Amministrazioni di eseguire test mirati alle applicazioni di tipo mobile consentendo la rilevazione delle vulnerabilità di sicurezza che possono essere sfruttate da un attaccante per compromettere i dati delle mobile app, la logica di business o il framework del dispositivo mobile identificando qualsiasi minaccia che mette a rischio l'applicazione e/o l'infrastruttura.

Si noti esplicitamente 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.

Il Fornitore, nell'ambito del servizio "Testing 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 la 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 ottimizzazioni da apportare;
- analisi e gestione delle policy di accesso ai dati e alle funzioni del dispositivo.

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:

- compatibilità con almeno i seguenti principali sistemi operativi: Android e iOS.

3.5.2 Metrica e modalità di remunerazione

La metrica del servizio di "Testing del codice - mobile" è:

- **numero di applicazioni/anno**

secondo le seguenti fasce:

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

La modalità di remunerazione del servizio "Testing del codice - mobile" 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.

3.6 L2.S21 - Supporto all'analisi e gestione degli incidenti

3.6.1 Requisiti tecnico-funzionali del servizio

Il servizio "Supporto all'analisi e gestione degli incidenti" dovrà consentire alle Amministrazioni e agli organismi deputati alle attività di prevenzione, supporto nello svolgimento delle attività di analisi degli incidenti e di divulgazione delle informazioni in caso di emergenza.

Il servizio è atto a garantire e supportare le Amministrazioni del rispetto e della corretta esecuzione di tutti i processi di gestione degli incidenti di sicurezza e di escalation.

Il servizio, a fronte di un incidente di sicurezza, dovrà prevedere attività volta a definire il livello di impatto, delle strutture ed entità da coinvolgere e delle contromisure da adottare; in particolare:

- la creazione e gestione di un piano di risposta agli incidenti (IRP);
- l'investigazione e analisi degli incidenti;
- 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;
- analisi dei log e degli eventi;
- malware forensic;
- network e system forensic;
- supporto ai processi di escalation verso le entità interne ed esterne (inclusi 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-incident per modifiche a tecnologia.

Si riportano di seguito, a titolo indicativo e non esaustivo, le attività di natura "consulenziale" del servizio:

- supporto alla incident management strategy, ossia definizione delle azioni di contenimento, modalità di gestione del rapporto con le entità interne ed esterne, ecc;
- supporto alla redazione e aggiornamento delle procedure di incident management richiamate nel processo di Incident Management emesso e gestito nell'ambito dei processi dell'Amministrazione in coerenza con le prassi e gli standard emessi del CSIRT-Italia;
- supporto alle Amministrazioni di cui al D.lgs 65/2018 per le attività di notifica degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti;
- supporto alla 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 ai 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).

3.6.2 Team di lavoro

Per erogare il presente servizio il fornitore dovrà disporre delle competenze, esperienze e capacità richieste ai profili professionali indicati nel seguito, che devono, tutte, **obbligatoriamente** fare parte del Team di Lavoro (o Team Ottimale) del servizio.
Il Team di Lavoro è sotto la responsabilità e l'organizzazione del fornitore.
Profili Professionali previsti nel Team di Servizio Supporto all'analisi e gestione degli incidenti (per il dettaglio dei profili si rimanda all'Appendice 3B Profili Professionali)

- Security Principal
- Senior Security Analyst
- Junior Security Analyst
- Forensic Expert

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

3.6.3 Metrica e modalità di remunerazione

La metrica del servizio di "Supporto all'analisi e gestione degli incidenti" è:

- **giorni/persona**

La modalità di remunerazione del servizio di "Supporto all'analisi e gestione degli incidenti" è:

- **progettuale (a corpo)**

3.7 L2.S22 - Penetration testing

3.7.1 Requisiti tecnico-funzionali del servizio

Il servizio di "Penetration testing" dovrà fornire alle Amministrazioni un processo operativo di analisi e valutazione dei punti deboli relativi ad una infrastruttura IT.

Il servizio, condotto su più fasi e mediante l'adozione di adeguati strumenti, si configura nella simulazione di un attacco informatico al sistema da parte di un utente malintenzionato al fine di rilevare la presenza di eventuali falle e vulnerabilità al suo interno. Verranno fornite il maggior numero di informazioni 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 esemplificativo vengono di seguito indicate le eventuali vulnerabilità utilizzabili a scopi malevoli:

- **vulnerabilità interne al sistema**: che permetterebbero 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 deriverebbero da pratiche non sicure nella esecuzione di un'applicazione, di un sito web, di un APP.
- **vulnerabilità delle reti wireless: che permetterebbero l'accesso a** dispositivi non autorizzati che fanno parte dell'ambiente protetto dell'organizzazione accesso e i dispositivi non autorizzati che fanno parte dell'ambiente protetto dell'organizzazione.
- **vulnerabilità delle API:** relative al corretto funzionamento delle logiche applicative soprattutto per quanto riguarda le meccaniche di autenticazione e autorizzazione.
- **vulnerabilità degli IoT:** relative al corretto funzionamento di tali infrastrutture allo scopo di estrarre informazioni o comprometterne il funzionamento.
- **vulnerabilità dei dati sensibili dovute ad un attacco di phising (Phishing):** relative alla valutazione della suscettibilità dei dipendenti agli attacchi di "ingegneria sociale"**.**

Le vulnerabilità possono quindi 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.

Di seguito le fasi che il servizio di "penetration testing" dovrà prevedere sono almeno le seguenti fasi:

Information gathering: l'obiettivo di questa fase è la 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: l'obiettivo di questa fase è stabilire un accesso al sistema, aggirando gli eventuali sistemi e controlli di sicurezza presenti. In questa fase il servizio potrà anche identificare nuove vulnerabilità e codificarne gli exploit.

Post Exploitation: l'obiettivo di questa fase consiste nella raccolta delle informazioni ottenute (comprese le password) e dei privilegi acquisiti durante la fase di Exploitation.

Reporting: l'obiettivo di questa fase è la preparazione di report, affinché sia evidente quali azioni sono state intraprese all'interno del perimetro definito, con quali motivazioni e con quali risultati, con le evidenze per cui sia possibile ricostruire e ripercorrere i percorsi intrapresi per sfruttare le vulnerabilità rilevate.

Il servizio di "Penetration testing" dovrà poter essere eseguito nelle seguenti modalità a scelta dell'Amministrazione:

White Box: il test presuppone conoscenze dettagliate dell'infrastruttura da esaminare, quali documentazione dell'architettura, gli schemi di rete, codice sorgente delle applicazioni e liste di indirizzi IP presenti nella rete. Mediante le informazioni che vengono fornite all'esaminatore 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 gli esaminatori 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.

3.7.2 Team di lavoro

Per erogare il presente servizio il fornitore dovrà disporre delle competenze, esperienze e capacità richieste ai profili professionali indicati nel seguito, che devono, tutte, **obbligatoriamente** fare parte del Team di Lavoro (o Team Ottimale) del servizio.
Il Team di Lavoro è sotto la responsabilità e l'organizzazione del fornitore.
Profili Professionali previsti nel Team di Servizio Penetration Testing (per il dettaglio dei profili si rimanda all'Appendice 3B Profili Professionali)

- Security Principal
- Senior Penetration tester
- Junior Penetration tester
- Forensic Expert

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

3.7.3 Metrica e modalità di remunerazione

La metrica del servizio di “Penetration Testing” è:

- **giorni/persona**

La modalità di remunerazione del servizio di “Penetration Testing” è:

- **progettuale (a corpo)**

3.8 L2.S23 - Compliance normativa

3.8.1 Requisiti tecnico-funzionali del servizio

Il servizio di "Compliance normativa" dovrà consentire alle Amministrazioni un supporto nell'attuazione degli adempimenti del GDPR (General Data Protection Regulation - Regolamento UE 2016) applicato all'ambito del perimentro IT.

Il servizio basato su un approccio metodologico, dovrà prevedere senza oneri aggiuntivi per l'Amministrazione l'adozione di strumenti e la presenza di competenze specifiche ed è volto a sviluppare un Sistema di gestione della Privacy che:

- garantisca all'Amministrazione l'adozione di un processo per assicurare e mantenere la conformità alla normativa sul lungo periodo;
- sia capace di porre in essere le azioni necessarie per garantire la mitigazione del rischio di non conformità;
- consenta di trasformare la privacy da un adempimento di legge ad un abilitatore "mandatorio", mediante un'analisi del modello di maturità dei processi di trattamento dei dati;

Il servizio di "Compliance normativa", in relazione al perimetro IT dell'Amministrazione, dovrà inoltre consentire:

- la valutazione delle principali fonti di rischio di non conformità cui l'Amministrazione è soggetta. Individuazione quindi delle norme, regole e i principi rilevanti per l'Amministrazione e traduzione di tali leggi in regole e procedure che dovranno guidare lo svolgimento dell'operatività della stessa. In tale ambito dovrà essere posta l'attenzione ogni volta che vengono emessi una nuova normativa, un nuovo regolamento o un nuovo standard al quale attenersi, da parte delle istituzioni, delle associazioni di categoria, degli organismi di vigilanza o dell'Amministrazione stessa;
- la raccolta e analisi della documentazione disponibile e delle eventuali evidenze/aree di approfondimento;
- la verifica tramite assessement della situazione corrente, 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 per i diversi macro ambiti (es. governance, processi e metodologie, IT/sicurezza);
- la definizione delle politiche e le procedure che dovranno essere poste in essere 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, qualora non siano risultati sufficienti/adeguati;
- 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'Ammnistrazione.

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;
- individuazione e aggiornamento del perimetro dei sistemi IT interessati dal regolamento GDPR;
- predisposizione della mappatura tra la classificazione dei dati trattati, i requisiti tecnici associati e le soluzioni tecnologiche a supporto al fine di garantire:
  - un livello minimo di sicurezza per tutti gli applicativi (baseline di sicurezza applicata a tutti i sistemi);
  - individuazione e applicazione di misure aggiuntive specifiche in base alla natura e criticità del dato, quali mascheramento, cifratura dei Data base, strong authetication, pseudonymisation;
- identificazione dei sistemi che raccolgono i consensi al trattamento dati di soggetti esterni ed interni; valutare la compliance rispetto alla normativa; definire e monitarare eventuali piani di rientro;
- predisposizone di modelli per la documentazione tecnica da produrre verso l'Autorità Garante e gli interessati in caso di data breach;
- supporto per l'identificazione ed il monitoraggio del Piano complessivo di interventi IT volti a garantire la compliance al GDPR;
- elaborazione 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 Assessement e Gap Analisys;
- piano degli interventi;
- registro dei trattamenti;
- scheda per il censimento dei trattatmenti
- 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.

3.8.2 Team di lavoro

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

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

Profili Professionali previsti nel Team di Servizio Compliance normativa (per il dettaglio dei profili si rimanda all'Appendice 3B Profili Professionali)

- Security Principal
- Data Protection Specialist
- Junior Information Security Consultant
- Senior Information security Consultant
- Senior security auditor

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

3.8.3 Metrica e modalità di remunerazione

La metrica del servizio di “Compliance normativa” è:

- **giorni/persona**

La modalità di remunerazione del servizio di “Compliance normativa” è:

- **progettuale (a corpo)**

4 ATTIVITA' PROPEDEUTICHE

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

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

In questo ambito trovano applicazione le regole relative agli indicatori di qualità riportati nell'Appendice 3A Indicatori di Qualità.

4.1 Attività propedeutiche all'erogazione dei servizi

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

Il Piano di Presa in carco dovrà contenere il dettaglio delle attività che devono essere espletate ad inizio contratto, l'impegno delle risorse professionali impiegate, la relativa pianificazione temporale, le attività, gli strumenti offerti per le fasi di:

- predisposizione della documentazione, degli strumenti oggetto di fornitura nonchè migliorie offerte (obbligatorio);
- acquisizione del know how del contesto organizzativo tecnico e funzionale dell'Amministrazione, ove richiesto dalla stessa.

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

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

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

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

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

- data a cui si riferisce lo stato di avanzamento;
- percentuale di avanzamento delle singole attività;

- razionali di ripianificazione, preventivamente concordate con la Amministrazione, scostamento eventuale delle date, dell'impegno e del volume;
- vincoli/criticità e relative azioni da intraprendere e/o intraprese.

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

Il mancato rispetto, nel corso dell'esecuzione del singolo contratto esecutivo, delle scadenze riportate nel Piano di Presa in carico comporterà l'applicazione dell'indicatore "SLSC – Slittamento di una scadenza contrattuale" dell'Appendice 3A.
Di seguito vengono descritte in dettaglio le singole fasi del processo complessivo.

4.2 Presa in carico

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

- configurazione del Portale della Fornitura per il Contratto esecutivo;
- predisposizione e configurazione degli eventuali strumenti tecnologici richiesti e offerti;
- predisporre la documentazione relativa alle modalità di misurazione degli Indicatori di Qualità.

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

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

Per tali attività Il Fornitore dovrà partecipare ad uno specifico addestramento erogato dall'Amministrazione o da terzi indicati dall'Amministrazione. Tale addestramento potrà consistere, ad esempio, in riunioni di lavoro, esame della documentazione esistente con assistenza di personale esperto, affiancamento nelle fasi esecutive.

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

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

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

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

Le attività di Presa in carico dovrà essere eseguita dal Fornitore nel rispetto dei tempi contrattualmente indicati pena l'applicazione della penale di cui all'Appendice 3A Indicatori di Qualità.

4.3 Trasferimento Know-how

Il Fornitore dovrà predisporre un Piano di Trasferimento per le attività di passaggio di consegne di fine fornitura (*phase-out*) con il trasferimento all'Amministrazione o a terzi da essa indicati, del know-how e delle competenze maturate nella conduzione dei servizi oggetto del Contratto esecutivo.
Il phase out, o transizione in uscita, consiste nelle seguenti attività da considerarsi come requisiti minimi:

- "passaggio di consegne" nei quali si gestiscano sistemi delle amministrazioni;
- "consegna dei dati dell'Amministrazione";
- "consegna della documentazione tecnica" completa e aggiornata allo stato dell'arte dei servizi.

Il passaggio di consegne di fine fornitura dovrà essere erogato dal Fornitore nel corso dell'ultimo mese di vigenza contrattuale del Contratto esecutivo, secondo la pianificazione concordata, senza alcun onere per l'Amministrazione.
Il Fornitore dovrà mettere a disposizione un apposito gruppo di lavoro dedicato, con un numero adeguato di risorse professionali, strumenti organizzativi e tecnologici, anche in relazione a quanto ulteriormente richiesto dall'Amministrazione e previsto in sede di offerta tecnica.

Si fa presente che il trasferimento di know-how potrà essere richiesto anche durante l'erogazione dei servizi nel corso della durata contrattuale, direttamente al personale dell'Amministrazione.
Sono incluse nelle attività di trasferimento:

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

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

- Durata massima delle attività di trasferimento: un mese di calendario continuativo dalla data di avvio del trasferimento che sarà indicata dall'Amministrazione.
- Per tutta la durata del trasferimento il Fornitore continuerà ad erogare i servizi di propria pertinenza.
- Predisposizione del Piano di Trasferimento: Il Piano di trasferimento (PTF) è un documento che prevede i seguenti contenuti minimi:
    - l'oggetto del trasferimento;
    - le attività e le relative modalità di esecuzione;

- i compiti e le responsabilità di ciascuna delle Parti;
- il programma temporale in base al quale le attività dovranno essere eseguite;

Il PTF sarà redatto dal Fornitore e sottoposto all'approvazione dell'Amministrazione almeno tre mesi prima della scadenza del Contratto esecutivo, ovvero entro il mese successivo alla data di comunicazione dell'evento che ne comporterà la cessazione anticipata. Il documento prodotto dovrà essere gestito dal Fornitore ed aggiornato a seguito delle modifiche richieste dall'Amministrazione ovvero intervenute nel corso di svolgimento delle attività di trasferimento (ad esempio a seguito del riesame congiunto con il Fornitore Subentrante nella fase di subentro, o anche successivamente durante lo svolgimento delle attività di trasferimento per aggiunta/modifica o cancellazione di attività/riunioni).

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

Il piano conterrà il dettaglio delle singole riunioni relative a tutte le fasi del progetto di trasferimento. Nella redazione del PTF occorre tener conto delle priorità, delle scadenze istituzionali e degli adempimenti tecnico amministrativi dell'Amministrazione.
La responsabilità della gestione contrattuale viene mantenuta dal Fornitore fino al termine delle attività di trasferimento del servizio specifico (o parte di esso) in conformità di quanto previsto dal PTF.

4.4 Modalità di attivazione dei servizi

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

Nel caso in cui l'Amministrazione fruisca di analoghi servizi preesistenti, il Fornitore dovrà esplicitamente prevedere, congiuntamente con l'Amministrazione contraente, le procedure di attivazione necessarie a garantire il mantenimento dell'operatività durante le fasi di migrazione. Eventuali necessità di fermo dei servizi devono essere accuratamente definite dal Fornitore, approvate dall'Amministrazione e monitorate in modo da ridurre al minimo gli impatti sull'utenza di riferimento.

Si precisa inoltre che in fase di avvio dell'erogazione dei servizi, il Fornitore dovrà sottoscrivere un accordo di riservatezza che lo impegna a non divulgare nessuna informazione relativa all'Amministrazione contraente, alle sue infrastrutture informatiche e ai suoi dati.

4.5 Eventuali attività di installazione per l'erogazione dei servizi

In relazione ad eventuali attività di installazione/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 intervalli orari definiti dall'Amministrazione contraente, coerentemente con le proprie esigenze di operatività;

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

Qualora un'operazione di installazione dovesse costituire causa di disservizio, il Fornitore dovrà adoperarsi per garantire il ripristino immediato della condizione preesistente (procedura di *roll-back*).

A partire dalla data di decorrenza del Contratto esecutivo, il Fornitore dovrà procedere all'installazione secondo le modalità temporali previste dal Piano Operativo; per tale attività e per le eventuali successive attività di configurazione il Fornitore, congiuntamente con l'Amministrazione, dovrà:

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

4.6 Team da impiegare nell'affidamento

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 documento e all'Appendice 3B "Profili Professionali", integrati con tutte le migliorie offerte in Offerta Tecnica.

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

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

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

I vincoli temporali sotto riportati, unitamente a quanto previsto contrattualmente, devono essere considerati come scadenze contrattuali e dunque presidiati dagli indicatori di cui all'Appendice 3A Indicatori di Qualità.

Vincoli temporali			
Attività	**Evento**	**Giorni**	**Note**
Pubblicazione sul Portale dei CV risorse PRESA IN CARICO e dei referenti tecnici	Stipula	5 giorni lavorativi	Allegato al piano di PRESA IN CARICO

Vincoli temporali			
Attività	**Evento**	**Giorni**	**Note**
Pubblicazione sul Portale dei CV delle risorse professionali e dei ruoli di interfaccia con l'Amministrazione	Stipula	10 giorni lavorativi	Allegato al piano di lavoro generale
Colloquio	Richiesta di colloquio	3 giorni lavorativi	
Disponibilità della risorsa nei team di lavoro	Comunicazione dell'esito positivo del colloquio	3 giorni lavorativi	In funzione degli specifici piani approvati
Pubblicazione sul Portale dei CV a valle di una valutazione di non idoneità di una risorsa/sostituzione	Valutazione di non idoneità un CV/ Sostituzione risorsa	3 giorni lavorativi	
Disponibilità della risorsa in sostituzione	Comunicazione di valutazione positiva	3 giorni lavorativi	In funzione degli specifici piani approvati

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

4.7 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.

Il Fornitore prende atto che le Amministrazioni potranno introdurre variazioni dell'ambito tecnologico, a fronte di specifiche esigenze dell'Amministrazione stessa o per le naturali evoluzioni dei programmi e dei sistemi ICT, e pertanto si impegna ad erogare i servizi adeguando le conoscenze del personale impiegato o inserendo nei gruppi di lavoro risorse con skill idonei allo svolgimento delle attività, senza alcun onere aggiuntivo per l'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 3B "Profili Professionali" sono indicate le competenze, le conoscenze e le relative certificazioni/credenziali delle risorse professionali che dovranno essere impiegate dal Fornitore per l'esecuzione della fornitura.

5 MODALITÀ DI EROGAZIONE

5.1 Comunicazioni e Approvazioni

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

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

Si precisa che la mancata approvazione di documenti contrattuali (inclusi i deliverable dei servizi) costituisce inadempimento contrattuale cui può conseguire l'adozione delle azioni contrattuali indicate nell'Appendice 3A Indicatori di Qualità.

5.2 Modalità di Approvazione

Tutte le comunicazioni inerenti l'approvazione (o mancata approvazione) dei prodotti della fornitura saranno notificati tramite il Portale. In nessun caso l'approvazione potrà avvenire per tacito assenso.

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

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

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

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

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

5.3 Verifiche di conformità

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

5.4 Azioni contrattuali

Ogni inadempimento contrattuale darà origine ad un'azione commisurata alla criticità dell'inadempimento stesso. I principali aspetti delle prestazioni contrattuali vengono presidiati da appositi indicatori di qualità.
Pertanto, il mancato rispetto dei requisiti minimi richiesti e/o migliorati dal fornitore in Offerta tecnica determina azioni contrattuali conseguenti che possono consistere in una o più delle seguenti azioni:

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

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

5.4.1 Rilievi

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

I rilievi non prevedono di per sé l'applicazione di penali, ma costituiscono avvertimento sugli aspetti critici della fornitura e, se reiterati e accumulati, danno luogo a penali, secondo quanto previsto in Appendice 3A Indicatori di Qualità.

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

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

5.4.2 Penali

Lo scopo delle penali è riequilibrare il servizio effettivamente ricevuto (di minore qualità, e/o generando disservizi e/o ritardi e/o inducendo un danno all'utilizzatore) dalla Amministrazione al corrispettivo da erogarsi che è stabilito per prestazioni effettuate nel rispetto dei requisiti.

5.5 Monitoraggio

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

La funzione di monitoraggio sarà svolta dalla Amministrazione o da soggetto da essa incaricato.
Il fornitore si impegna a fornire all'Amministrazione tutti i documenti necessari all'attività di monitoraggio nei formati richiesti e necessari per il controllo e la verifica della fornitura, salvo evoluzioni derivanti dall'introduzione, da parte della Amministrazione, di strumenti automatici a ciò deputati.

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

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

5.6 Team di Lavoro

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

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

I Profili Professionali previsti nei Team sono i seguenti (per il dettaglio dei profili si rimanda all'Appendice 3B Profili Professionali:

- Security Principal
- Senior information security consultant
- Junior information security consultant
- Security solution architect
- Senior security auditor
- Senior security analist
- Junior security analist
- Senior penetration tester
- Junior penetration tester
- Forensic expert
- Data protection specialist

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

L'importo del servizio è determinato sulla base dei giorni/team definiti dall'Amministrazione nel Piano dei Fabbisogni.

Il Fornitore sarà libero di organizzare le suddette figure nell'ambito del proprio Team Ottimale in autonomia per soddisfare le richieste progettuali dell'Amministrazione, garantendo in ogni caso il rispetto delle scadenze previste, degli indicatori di qualità ed il livello atteso dei deliverables di fornitura.

Ai fini della remunerazione a corpo, il Fornitore sarà libero di organizzare le suddette figure nell'ambito del proprio "team ottimale" per singolo servizio. L'Amministrazione in ogni caso avrà la possibilità, nella fase di esecuzione dei servizi, di verificare l'effettiva presenza di tali figure nel team di lavoro dedicato all'erogazione dei servizi.

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

5.7 Dimensionamento dei servizi

5.7.1 Progettuale (a corpo)

Per i servizi con dimensionamento progettuale (a corpo) la responsabilità del risultato è affidata al Fornitore, il quale organizza le proprie risorse professionali, tecniche e metodologiche per soddisfare le richieste dell'Amministrazione. L'Amministrazione fornisce le macro esigenze partendo dal contesto funzionale e tecnologico.

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

Con l'approvazione del piano di lavoro, il Fornitore ne è responsabile, e, pertanto, non potrà richiedere maggiori costi o tempi per le attività previste. Il Fornitore inoltre risponderà dei danni causati da errata allocazione delle risorse o incompetenza delle risorse, mancata comprensione delle richieste dell'Ammninistrazione, mancato rispetto delle linee guida tecnologiche e dei livelli di qualità, ecc., e, dovrà rimediare a proprie spese per erogare una prestazione conforme funzionalmente e tecnicamente ai requisiti approvati.

5.7.2 Continuativa (a canone)

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

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

Tali servizi vengono erogati senza soluzione di continuità, sulla base delle frequenze temporali stabilite nella presente Appendice 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.

5.8 Pianificazione e Consuntivazione

5.8.1 Piano della Qualità Generale

Il Piano della Qualità Generale è descritto nelle Condizioni di fornitura.

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

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

5.8.2 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 a i servizi e sia le eventuali deroghe da quanto previsto nel Piano della Qualità Generale. Nel caso in cui per un determinato capitolo non ci siano differenze rispetto al Piano di Qualità Generale dell'AQ occorre solo riportare il riferimento al suddetto piano.

1. Descrizione specifica del Contratto esecutivo
2. Scopo del Piano della Qualità

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

3. Documenti applicabili e di riferimento
4. Ruoli e Responsabilità di riferimento
5. Modalità di erogazione, consuntivazione dei servizi
6. Metodi, tecniche e strumenti specifici del servizio/attività

(Contiene l'indicazione dei metodi, delle tecniche, degli strumenti, degli standard di prodotto specifici del servizio solo se diversi da quelli descritti nel Piano della Qualità Generale dell'AQ)

7. Indicatori di qualità specifici del servizio

(Contiene gli attributi di qualità con riferimento alle metriche, ai valori limite-Valore di soglia-definiti negli indicatori di qualità)

8. Riesami, verifiche e validazioni

(Contiene l'elenco dei controlli da effettuare per il servizio e le modalità di esecuzione dei controlli comprensive sia degli strumenti da utilizzare e sia della modulistica di rendicontazione dei risultati, se diversi da quelli descritti nel Piano della Qualità Generale).

5.8.3 Piani di Lavoro

Il Fornitore dovrà predisporre, con le tempistiche indicate nel Condizioni di fornitura, e mantenere costantemente aggiornata la pianificazione dei servizi/attività, con la seguente articolazione:
Piano di lavoro generale comprensivo di:

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

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

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

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

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

5.8.4 Stato Avanzamento Lavori

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

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

5.8.5 Consuntivazione

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

Il piano di lavoro dovrà essere corredato dal Rendiconto Risorse.

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

5.9 Orario di erogazione dei servizi

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

Tabella Orario di erogazione dei servizi

Servizi	Orario
Impiego delle figure professionali	Lunedi – Venerdi: 08:30 – 17:30 Sabato (festivi esclusi): 08:30 – 14:00

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

Si precisa che:

- è ammessa una flessibilità di 30 minuti sull'orario di inizio/fine di erogazione;
- la copertura temporale potrà essere differenziata per servizio indicando le modalità nel piano di lavoro;
- in caso sia presente un team di lavoro l'orario sarà garantito secondo una distribuzione delle presenze, eventuale turnazione delle risorse a copertura dell'intero orario, da concordare con l'Amministrazione nel piano di lavoro. All'interno dell'orario di servizio, non sono previste maggiorazioni;
- relativamente all'extraorario pianificato (oltre le ore 17,30 – dal lunedì al venerdì ed oltre le ore 14:00 il sabato) nonché domenica e festivi, gli interventi (on-site o da remoto) verranno retribuiti alla tariffa oraria base maggiorata del 20%;
- per festività devono intendersi solamente le festività a carattere nazionale e le domeniche, salvo casi indicati dall'Amministrazione in cui non vi siano servizi attivi.
- la tariffa oraria è data dalla tariffa giornaliera offerta (riferita a 8 ore lavorative) diviso 8;

Può essere necessario, in relazione a esigenze dell'Amministrazione, non sempre prevedibili con la pianificazione mensile, un prolungamento dell'orario, all'interno delle fasce di cui alla Tabella precedente, dei servizi o la disponibilità di servizio il sabato. La disponibilità alla richiesta di estensione dell'orario di servizio suddetto è da considerare già remunerata nel corrispettivo globale della fornitura.

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

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

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

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

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