



Classificazione Consip: Ambito Pubblico

Capitolato tecnico – Parte Speciale

GARA A PROCEDURA APERTA AI SENSI DEL D. LGS. 36/2023 E S.M.I., PER L’AFFIDAMENTO DI SERVIZI PROFESSIONALI PER LA GESTIONE E CONDUZIONE DI INFRASTRUTTURE DI CYBERSECURITY DELLE PA – LOTTI 1 E 2

ID 2909

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

Capitolato Tecnico Speciale

Indice

1	PREMESSA	6
1.1	Scopo del documento	6
1.2	Oggetto	7
	1.2.1 Articolazione degli ambiti e dei servizi	8
2	DESCRIZIONE DEI SERVIZI	9
2.1	Supporto operativo all'Assessment Tecnologico (Asset Inventory)	11
	2.1.1 Attività previste	12
	2.1.2 Deliverable	13
	2.1.3 Figure professionali coinvolte	15
	2.1.4 Metrica di dimensionamento e modalità di remunerazione	15
2.2	Presidio di event e incident management	16
	2.2.1 Disposizioni generali del servizio	17
	2.2.2 Attività previste	18
	2.2.3 Deliverable	24
	2.2.4 Figure professionali coinvolte	28
	2.2.5 Metrica di dimensionamento e modalità di remunerazione	28
2.3	Continuous Vulnerability Management	28
	2.3.1 Attività previste	29
	2.3.2 Deliverable	35
	2.3.3 Figure professionali coinvolte	38
	2.3.4 Metrica di dimensionamento e modalità di remunerazione	39
2.4	Sicurezza dei sistemi e delle applicazioni	39
	2.4.1 Attività previste	40

2.4.2	Deliverable	59
2.4.3	Figure professionali coinvolte	61
2.4.4	Metrica di dimensionamento e modalità di remunerazione	62
2.5	Conduzione operativa dei sistemi di sicurezza	62
2.5.1	Attività previste	63
2.5.2	Deliverable	65
2.5.3	Figure professionali coinvolte	67
2.5.4	Metrica di dimensionamento e modalità di remunerazione	67
2.6	Supporto specialistico	68
2.6.1	Attività previste	68
2.6.2	Deliverable	73
2.6.3	Figure professionali coinvolte	75
2.6.4	Metrica di dimensionamento e modalità di remunerazione	75
2.7	Gestione accessi e identità	76
2.7.1	Attività previste	76
2.7.2	Deliverable	79
2.7.3	Figure professionali coinvolte	81
2.7.4	Metrica di dimensionamento e modalità di remunerazione	81
2.8	Formazione tecnica	82
2.8.1	Metrica di dimensionamento e modalità di remunerazione	84
3	RISORSE DA IMPIEGARE NELL'ESECUZIONE DEI SERVIZI	85
3.1.1	Security Principal	89
3.1.2	Security Architect	91
3.1.3	Cloud Security Expert	93
3.1.4	OT/IoT Security Expert	95

3.1.5	Senior Security Consultant	97
3.1.6	Forensics Expert	99
3.1.7	Security Analyst	100
3.1.8	Security Specialist	101
3.1.9	Junior Security Consultant	103
3.1.10	Legal, Policy and Compliance Officer	105
3.1.11	Threat intelligence specialist	108
3.1.12	Incident responder	109
3.1.13	Information Security Manager	111
3.1.14	Senior Penetration Tester	112
3.1.15	Junior Penetration Tester	115
3.1.16	AI Security Specialist	117
3.1.17	Security Engineer	119
3.1.18	Network Security Engineer	121
3.1.19	Valutazione dei curricula	122
4	INDICATORI DI QUALITÀ	124
4.1	IQ01 – Rispetto di una scadenza contrattuale	124
4.2	IQ02 – Adeguatezza delle figure professionali proposte per la erogazione dei servizi	126
4.3	IQ03 – Adeguatezza del personale impiegato nei ruoli contrattuali	127
4.4	IQ04 – Adeguatezza dei tempi di sostituzione delle figure professionali proposte per la erogazione dei servizi	128
4.5	IQ05 - Turnover del personale impiegato nella fornitura	129
4.6	IQ06 – Impegni assunti in offerta tecnica	130
4.7	IQ07 – Tempestività di risposta per il servizio di Service Desk	131
4.8	IQ08 – Qualità complessiva dell’Asset Inventory	132
4.9	IQ09 – Tempestività di presa in carico del supporto di Incident ed Event Management	134

4.10	IQ10 – Qualità del triage e della classificazione degli eventi	135
4.11	IQ11 – Conformità del supporto alle procedure dell'Amministrazione	137
4.12	IQ12 – Efficacia del supporto specialistico senza ulteriore escalation	138
4.13	IQ13 – Completezza delle evidenze tecniche per decisioni e notifiche	139
4.14	IQ14 – Copertura del perimetro assegnato	140
4.15	IQ15 – Completezza delle attività di sicurezza applicativa e infrastrutturale	142
4.16	IQ16 – Conformità del modello di gestione delle identità (IAM)	144
4.17	IQ17 – Efficacia delle attività di bonifica IAM	145
4.18	IQ18 – Completezza dei deliverable di Supporto specialistico	146
4.19	IQ19 – Erogazione dei moduli di formazione tecnica	147
4.20	IQ20 – Efficacia della formazione tecnica	148
4.21	IQ21 – Conformità dei docenti e della documentazione formativa	149
4.22	IQ22 – Rilievi su obbligazioni contrattuali non presidiate	151
5	SCHEMA PER LA PRESENTAZIONE DEI CURRICULA	152

Indice delle tabelle

Tabella 1. Esperienza aggiuntiva da considerare come “cultura equivalente”	87
--	----

1 PREMESSA

1.1 Scopo del documento

Il presente Capitolato Tecnico Speciale disciplina le modalità di erogazione dei **servizi professionali di cybersecurity** oggetto della procedura di gara **ID 2909**, finalizzati a supportare le Pubbliche Amministrazioni nella **gestione operativa, nel presidio e nel rafforzamento della postura di sicurezza** delle infrastrutture tecnologiche già in esercizio.

I servizi sono orientati a fornire **supporto specialistico continuativo e attività di staff augmentation**, mediante l'impiego di risorse qualificate, operanti in modalità **autonoma o integrata** con le strutture dell'Amministrazione, al fine di garantire:

- continuità operativa dei sistemi e dei servizi critici;
- capacità di prevenzione, rilevazione e risposta agli eventi di sicurezza;
- adeguamento progressivo al quadro normativo e regolatorio di riferimento in materia di cybersicurezza.

Il Capitolato definisce il perimetro tecnico dei servizi, gli ambiti di intervento, le modalità organizzative e operative, nonché i requisiti minimi di qualità, nel rispetto delle disposizioni previste dalla documentazione di gara e in coerenza con:

- le esigenze differenziate delle **Pubbliche Amministrazioni Centrali (PAC)** e delle **Pubbliche Amministrazioni Locali (PAL)**;
- i contesti di impiego connessi alla tutela degli interessi strategici e della sicurezza nazionale, ove applicabili;
- l'utilizzo prioritario delle infrastrutture e degli strumenti già in dotazione alle Amministrazioni.

Il presente Capitolato costituisce parte integrante della documentazione di gara per la descrizione tecnica dei servizi e delle modalità di esecuzione, restando inteso che eventuali indicatori, livelli di servizio e dimensionamenti saranno declinati negli specifici paragrafi.

Le prescrizioni contenute nel presente documento costituiscono **requisiti minimi della fornitura** per entrambi i lotti oggetto di appalto.

Conseguentemente:

- il mancato rispetto in fase di offerta comporta l'esclusione dalla procedura di gara;

- il mancato rispetto in fase esecutiva costituisce inadempimento contrattuale e comporta l'applicazione delle azioni contrattuali e delle penali previste.

Salvo diversa indicazione, **tutti i termini temporali riportati nel presente Capitolato sono da intendersi come giorni solari**. Ove espressamente indicato, i termini sono da considerarsi giorni lavorativi o ore lavorative, secondo quanto specificato nei singoli paragrafi e nei livelli di servizio (SLA), in coerenza con le definizioni di cui al Capitolato Tecnico Generale.

Si rinvia agli acronimi e alle definizioni riportati nel Capitolato Tecnico Generale.

1.2 Oggetto

L'oggetto della presente iniziativa riguarda l'affidamento di un panel di servizi professionali specialistici e trasversali di cybersecurity, finalizzati a supportare le Pubbliche Amministrazioni nel potenziamento della gestione operativa, nel presidio tecnico e nella capacità di reazione alle minacce di sicurezza, con riferimento alle infrastrutture di cybersecurity già in possesso delle Amministrazioni.

I servizi oggetto della fornitura sono articolati negli ambiti descritti nel presente Capitolato e costituiscono il perimetro tecnico dell'Accordo Quadro.

I servizi sono concepiti come servizi professionali di supporto tecnico, affiancamento operativo e staff augmentation, erogati mediante team autonomi o integrati nelle strutture dell'Amministrazione, e non si configurano come servizi gestiti né come outsourcing end-to-end delle funzioni di sicurezza.

L'erogazione dei servizi non comporta l'assunzione di responsabilità decisionali, di governo o di controllo autonomo da parte del Fornitore, che restano integralmente in capo all'Amministrazione, secondo i modelli organizzativi e i processi dalla stessa adottati.

I requisiti normativi applicabili, inclusi, ove pertinenti, quelli previsti dal DPCM 30 aprile 2025, dalle Linee guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) e dalla normativa vigente in materia di sicurezza informatica e protezione degli asset critici, per i quali si rinvia al Capitolato Tecnico Generale.

L'iniziativa non prevede l'acquisizione di prodotti, ma la sola erogazione di servizi professionali specialistici. Per tali servizi, il Fornitore potrà, ove necessario e previo accordo con l'Amministrazione, utilizzare propri strumenti esclusivamente ai fini dell'erogazione del servizio, senza oneri a carico dell'Amministrazione stessa.

1.2.1 Articolazione degli ambiti e dei servizi

I servizi oggetto della presente iniziativa sono organizzati in **ambiti funzionali omogenei**, ciascuno dei quali comprende uno o più servizi specialistici, tra loro coerenti per finalità, perimetro tecnico e modalità di erogazione.

In particolare, l'Accordo Quadro prevede i seguenti **ambiti di servizio**.

Asset Inventory

Ambito finalizzato al supporto operativo alle attività di assessment tecnologico e di inventariazione degli asset dell'Amministrazione, comprensivo dei servizi di supporto all'Asset Inventory e alle attività di mantenimento e aggiornamento delle informazioni sugli asset infrastrutturali, applicativi e tecnologici.

Presidio di event e incident Management

Ambito dedicato al supporto specialistico alla gestione degli eventi e degli incidenti di sicurezza informatica, comprensivo dei servizi di presidio operativo per la gestione degli incidenti, di supporto alle attività di triage, analisi, escalation, contenimento e supporto avanzato, secondo i livelli operativi previsti.

Continuous Vulnerability Management

Ambito finalizzato al governo continuo della superficie di attacco e della postura di sicurezza, comprensivo dei servizi di Vulnerability Assessment, Penetration Test, Red Team, Blue Team, Purple Team, analisi e integrazione delle evidenze di rischio, valutazione periodica della postura di sicurezza dell'Amministrazione e dei fornitori della stessa.

Sicurezza dei sistemi e delle applicazioni

Ambito dedicato al rafforzamento della sicurezza infrastrutturale e applicativa, comprensivo dei servizi di sicurezza applicativa (SAST, DAST, MAST), gestione dell'hardening delle soluzioni di sicurezza dell'Amministrazione, gestione del patching delle soluzioni di sicurezza e definizione di processi e procedure per la verifica dell'integrità dei sistemi.

Conduzione operativa dei sistemi di sicurezza

Ambito finalizzato alla gestione operativa sistemistica e applicativa dei sistemi e delle piattaforme di sicurezza dell'Amministrazione, comprensivo dei servizi di conduzione operativa ordinaria e su richiesta dei sistemi di sicurezza, nel rispetto delle configurazioni, delle policy e delle autorizzazioni definite dall'Amministrazione.

Supporto specialistico

Ambito trasversale e flessibile, finalizzato a fornire competenze professionali ad elevata specializzazione a supporto di esigenze puntuali o iniziative complesse, comprensivo dei servizi di supporto alla migrazione tecnologica, integrazione tecnologica, progettazione e revisione di architetture di cybersecurity e continuità operativa, nonché supporto specialistico per la sicurezza di soluzioni basate su tecnologie di intelligenza artificiale e machine learning.

Gestione accessi e identità

Ambito dedicato al supporto alla definizione e all'attuazione dei modelli operativi di gestione delle identità digitali e degli accessi logici, comprensivo dei servizi di formalizzazione dei modelli IAM e di supporto all'attuazione operativa dei processi di gestione degli accessi.

Formazione tecnica

Ambito finalizzato al trasferimento di competenze tecniche e operative al personale dell'Amministrazione, comprensivo dei servizi di formazione tecnica sull'utilizzo delle soluzioni e degli strumenti di cybersecurity adottati.

Il successivo Capitolo 2 descrive nel dettaglio gli ambiti di servizio e i relativi servizi che li compongono, specificandone obiettivi, attività, deliverable e figure professionali coinvolte.

2 DESCRIZIONE DEI SERVIZI

I servizi oggetto della presente iniziativa hanno l'obiettivo di mettere a disposizione dell'Amministrazione un **insieme integrato di capacità professionali e competenze specialistiche** prevalentemente tecniche e operative, finalizzate al rafforzamento della postura di sicurezza, alla gestione operativa dei controlli di cybersecurity.

L'intero portafoglio dei servizi è progettato per supportare l'Amministrazione nell'attuazione e nel mantenimento di un **sistema di sicurezza informatica coerente, strutturato e progressivamente evolutivo, in linea con gli indirizzi** dell'Agenzia per la Cybersicurezza Nazionale (ACN), con il quadro normativo vigente e con le esigenze di protezione delle infrastrutture ICT, delle applicazioni, dei dati e dei processi della Pubblica Amministrazione.

In tale contesto, i servizi descritti nel presente Capitolo dovranno consentire all'Amministrazione di:

- analizzare e comprendere il livello di esposizione al rischio delle componenti infrastrutturali, applicative e dei servizi digitali;
- supportare l'implementazione e il mantenimento di controlli tecnici e procedure operative di sicurezza, in coerenza con i requisiti normativi e regolatori applicabili e gli standard di settore;
- rafforzare le capacità di prevenzione, rilevazione, gestione e risposta agli eventi e agli incidenti di sicurezza informatica;
- verificare l'efficacia delle misure di sicurezza adottate e supportarne il miglioramento continuo;
- individuare i fabbisogni evolutivi in termini di servizi, competenze e tecnologie di sicurezza.

I servizi sono erogati in modalità di **supporto tecnico-specialistico e affiancamento operativo** alle strutture dell'Amministrazione, nel rispetto dei processi, delle policy e dei modelli organizzativi dalla stessa adottati, e non si configurano come servizi gestiti né come assunzione di responsabilità end-to-end da parte del Fornitore.

Il Fornitore opera sulla base delle specifiche esigenze rappresentate dall'Amministrazione, assicurando la disponibilità di risorse qualificate, adeguata flessibilità nell'impiego delle stesse e un'interlocuzione costante con le funzioni interne competenti, al fine di garantire la corretta integrazione delle attività nei processi esistenti e il raggiungimento degli obiettivi attesi.

Le attività di **governo complessivo, coordinamento metodologico, pianificazione trasversale e Program/Project Management** della fornitura non rientrano nel perimetro dei servizi disciplinati dal presente Capitolo. Per un supporto strutturato e metodologico alle attività di demand management, program management e project management, l'Amministrazione potrà fare riferimento ai **servizi di PMO resi disponibili nell'ambito dell'iniziativa Consip Digital Transformation** e definiti nella documentazione di gara. I servizi di cybersecurity descritti nel presente Capitolato si inseriscono in tale contesto di governo, fornendo contributi tecnici e specialistici coerenti con le pianificazioni e le priorità definite dall'Amministrazione. Le modalità di coordinamento tra i servizi di cui al presente Capitolato e le funzioni di governo, nonché le regole di interazione con i servizi di demand e PMO attivati nell'ambito dell'AQ Digital Transformation, sono disciplinate nel **Capitolato Tecnico Generale**, cui si rinvia.

L'erogazione dei servizi dovrà tenere conto del quadro normativo, organizzativo e tecnologico dell'Amministrazione, nonché delle sue caratteristiche dimensionali e del livello di complessità dei sistemi informativi. Considerata la natura critica delle attività, è richiesto un elevato livello di competenza tecnica, accuratezza operativa, riservatezza e capacità di risposta anche in situazioni di urgenza.

I servizi sono erogati nel rispetto dei requisiti definiti nel Piano della Qualità Generale dell'Iniziativa e nei Piani di Qualità dei singoli Contratti Esecutivi. Tutte le attività sono oggetto di preventiva condivisione con l'Amministrazione e di successiva validazione, anche ai fini del monitoraggio della qualità.

I deliverable prodotti devono essere immediatamente fruibili, tracciabili e conformi ai formati richiesti e devono essere resi disponibili in formati aperti, standardizzati e privi di restrizioni di interoperabilità, tali da consentirne il riuso, la modifica e l'integrazione da parte dell'Amministrazione o di soggetti terzi dalla stessa incaricati.

Resta fermo che eventuali dati, configurazioni, policy e parametri generati o gestiti nell'ambito dei servizi devono essere pienamente esportabili, senza oneri aggiuntivi, al fine di garantire la portabilità dei deliverable, la neutralità tecnologica e l'assenza di vincoli di lock-in.

Salvo diversa indicazione nei singoli paragrafi, le attività sono svolte principalmente presso le sedi dell'Amministrazione; su richiesta, possono essere svolte anche da remoto o presso le sedi del Fornitore, nel rispetto dei requisiti di sicurezza e riservatezza.

2.1 Supporto operativo all'Assessment Tecnologico (Asset Inventory)

Il servizio di **Supporto operativo all'Assessment Tecnologico (Asset Inventory)** consiste nell'erogazione di attività tecniche e operative per la rilevazione, classificazione, aggiornamento e normalizzazione degli **asset tecnologici dell'Amministrazione** (infrastrutturali, applicativi e, ove presenti, eventuali componenti OT/IoT).

Le attività vengono svolte utilizzando gli **strumenti già in uso presso l'Amministrazione**, che possono includere piattaforme strutturate (es. *CMDB – Configuration Management Database*, strumenti di discovery, sistemi di monitoraggio) oppure strumenti meno formalizzati (es. *repository condivisi, documentazione tecnica, fogli Excel*).

Ove necessario e **previo accordo con l'Amministrazione**, il Fornitore potrà integrare **propri strumenti** ai soli fini dell'erogazione del servizio, **senza oneri aggiuntivi**, quali, a titolo esemplificativo: script o tool di supporto per analisi/normalizzazione, strumenti di data quality, discovery o riconciliazione.

L'obiettivo è consolidare un inventario affidabile e aggiornato, a supporto delle attività tecniche di gestione, sicurezza e controllo.

2.1.1 Attività previste

Rilevazione e discovery degli asset

- Utilizzo degli strumenti già presenti presso l'Amministrazione quali:
 - o Sistemi di discovery (se presenti);
 - o CMDB – *Configuration Management Database* o altri strumenti di inventariazione dell'Amministrazione(inclusi fogli Excel);
 - o strumenti di monitoraggio o liste fornitori/dispositivi;
- Identificazione delle tipologie di asset (infrastrutturali, applicativi, di rete e, ove presenti, OT/IoT);
- Eventuale integrazione, ove necessario, con strumenti del Fornitore solo ai fini del servizio.

Raccolta e consolidamento delle informazioni

- Raccolta dati da tutte le fonti disponibili presso l'Amministrazione, si cita a titolo esemplificativo:
 - o inventari esistenti;
 - o documentazione tecnica;
 - o AD – Active Directory;
 - o esiti di VA/PT (se presenti);
 - o repository applicativi;
- Normalizzazione dei dati secondo gli standard definiti e concordati con l'Amministrazione.

Popolamento e aggiornamento degli strumenti dell'Amministrazione

- Aggiornamento delle informazioni negli strumenti dell'Amministrazione(CMDB, liste asset, fogli Excel, sistemi ITSM - *IT Service Management*);
- Validazione dei dati tramite riconciliazione con le fonti dell'Amministrazione.

Analisi di completezza e qualità del dato

- Identificazione di asset mancanti, duplicati, incoerenti;
- Segnalazione delle anomalie all'Amministrazione e supporto nella loro risoluzione;
- Aggiornamento delle informazioni negli strumenti dell'Amministrazione a valle delle verifiche.

Reportistica e dashboard tecniche

- Produzione di report tecnici su copertura, qualità del dato, gap inventariali;
- Produzione di **dashboard tecniche**, utilizzando strumenti dell'Amministrazione; in assenza, fornitura di dashboard in formato **stand-alone** (es. Excel, PDF, PowerBI locale).

Ulteriori attività richiedibili:

- Mappatura asset–servizi/processi.
- Formazione operativa sugli strumenti inventariali dell'Amministrazione (CMDB o fogli Excel).

- Integrazione con altri sistemi dell'Amministrazione (monitoring, SIEM, strumenti di VA/PT).
- Aggiornamento dell'inventario.

Inoltre, in caso di richieste di chiarimenti sull'operato da parte dell'Amministrazione, formalizzate attraverso i canali di comunicazione previsti o concordati nell'ambito del Contratto Esecutivo, il Fornitore dovrà fornire riscontro entro 2 giorni lavorativi.

Il Fornitore dovrà condurre **SAL periodici settimanali** (o con diversa periodicità concordata con l'Amministrazione) e produrre la relativa documentazione in formato:

- **dettagliato** per le strutture operative;
- **executive** per le strutture direttive.

2.1.2 Deliverable

I deliverable minimi attesi e le modalità/tempistiche di produzione sono:

ID	TITOLO	DESCRIZIONE	SLA
AI_1	Asset Inventory aggiornato	Inventario normalizzato degli asset tecnologici (estratto dagli strumenti dell'Amministrazione: CMDB, Excel, repository, etc)	Entro 30 giorni lavorativi dall'avvio delle attività, salvo diversa tempistica concordata con l'Amministrazione (in ogni caso non superiore ai 30 giorni).
AI_1.1	Asset Inventory aggiornato in itinere	Aggiornamento dell'inventario per variazioni critiche	Entro 48 ore lavorative dal rilevamento o dalla comunicazione dell'Amministrazione.
AI_2	Report di assessment	Report di assessment tecnologico con evidenza delle attività svolte, dei gap individuati e della loro risoluzione, ivi incluse le attività di riconciliazione svolte e i KPI di interesse, tra cui almeno: – Copertura asset identificati; – Accuratezza dati normalizzati; – Eliminazione incoerenze e duplicati.	Entro 20 giorni dalla chiusura delle attività di raccolta e normalizzazione dei dati, comprensivo dei KPI prima indicati.

ID	TITOLO	DESCRIZIONE	SLA
			Ad evento, entro 5 giorni dall'aggiornamento dell'Inventory.
AI_3	Dashboard	Dashboard di governance tecnica (su strumenti dell'Amministrazione o in formato stand-alone), con indicazione dei KPI di interesse, tra cui almeno: – Copertura asset identificati; – Accuratezza dati normalizzati; – Eliminazione incoerenze e duplicati.	Entro 5 giorni lavorativi successivi alla consegna del report di assessment.
AI_4	Documentazione di mapping asset-processi (Opzionale)	Documentazione tecnica che descrive la relazione tra gli asset tecnologici censiti e i servizi, i processi o le funzioni organizzative dell'Amministrazione, al fine di supportare le attività di analisi del rischio, continuità operativa e gestione della sicurezza. La documentazione è prodotta sulla base delle informazioni e delle classificazioni rese disponibili dall'Amministrazione e non comporta la definizione o la modifica dei processi organizzativi esistenti.	Entro 20 giorni lavorativi dall'avvio delle attività, salvo diversa tempistica concordata con l'Amministrazione (in ogni caso non superiore ai 20 giorni).
AI_5	Manuale operativo aggiornato per attività di discovery/CMDB (Opzionale)	Manuale operativo contenente le modalità di utilizzo, aggiornamento e manutenzione degli strumenti inventariali dell'Amministrazione (es. CMDB, repository, fogli di lavoro), comprensivo delle procedure di discovery, normalizzazione, riconciliazione e aggiornamento dei dati. Il manuale è finalizzato a supportare la continuità operativa delle attività di Asset Inventory da parte del personale dell'Amministrazione e non costituisce documentazione di prodotto o di piattaforma.	Entro 30 giorni lavorativi dall'avvio delle attività, salvo diversa tempistica concordata con l'Amministrazione (in ogni caso non superiore ai 30 giorni).

ID	TITOLO	DESCRIZIONE	SLA
AI_6	Risposte di chiarimento	Risposta alle richieste di chiarimento dell'Amministrazione	Entro 48 ore lavorative dalla comunicazione dell'Amministrazione
AI_7	SAL periodici	Il Fornitore dovrà produrre SAL, in formato: – dettagliato per le strutture operative; – executive per le strutture direttive.	Settimanali (o con diversa periodicità concordata con l'Amministrazione)

L'Amministrazione valuterà i deliverable entro **5 giorni lavorativi** dalla consegna. In caso di richieste di modifica, il Fornitore dovrà aggiornare/modificare i deliverable entro **5 giorni lavorativi** dalla comunicazione dell'Amministrazione, salvo diversa tempistica concordata.

Tutte le tempistiche dovranno essere indicate nel Piano di Lavoro Generale.

Gli adempimenti indicati nel presente paragrafo sono valutati ai fini di rilievi/penali in:

- 4.1 IQ01 – *Rispetto di una scadenza contrattuale;*
- 4.2 IQ02 – *Adeguatezza delle figure professionali proposte per la erogazione dei servizi;*
- 4.5 IQ05 - *Turnover del personale impiegato nella fornitura;*
- 4.6 IQ06 – *Impegni assunti in offerta tecnica;*
- 4.8 IQ08 – *Qualità complessiva dell'Asset Inventory;*
- 4.22 IQ22 – *Rilievi su obbligazioni contrattuali non presidiate.*

2.1.3 Figure professionali coinvolte

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 al capitolo 3 *Risorse da impiegare nell'esecuzione dei servizi*):

1. Security Principal;
2. OT/IoT Security Expert;
3. Security Analyst;
4. Security Specialist;
5. Information Security 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.

2.1.4 Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento di tutti i servizi è: **Giorno/Persona**.

La modalità di remunerazione di tutti i servizi è: **a tempo/spesa oppure a corpo**.

In fase di offerta è richiesto al Concorrente di esprimere un prezzo per giorno/persona per ogni figura professionale prevista. I prezzi espressi saranno riferiti rispettivamente a:

- 8 ore lavorative complessive nella fascia oraria feriale Lun-Sab 8.00-20.00 (fascia standard).

In sede di Piano dei fabbisogni, l'Amministrazione definirà i deliverables richiesti e le risorse necessarie, indicando quindi il mix necessario per le attività richieste, in un'ottica di coerenza e proporzionalità.

2.2 Presidio di event e incident management

Il Presidio di event e incident management è un **ambito funzionale** configurato come **presidio di supporto specialistico**, erogato mediante **l'innesto di risorse professionali singole o di gruppi organizzati del Fornitore** all'interno delle strutture operative dell'Amministrazione, al fine di supportare la gestione degli incidenti di sicurezza informatica.

Il Presidio non costituisce un SOC o un CSIRT autonomo del Fornitore, né un servizio esterno erogato in modalità "chiavi in mano", ma opera **in integrazione funzionale con il personale, i processi e gli strumenti dell'Amministrazione**.

Le risorse del Fornitore possono essere innestate, secondo le esigenze dell'Amministrazione e quanto previsto dal Piano dei Fabbisogni, **in una o più aree del processo di gestione degli incidenti**, tra cui a titolo esemplificativo e non esaustivo:

- strutture di monitoraggio e rilevamento (SOC);
- team di Incident Response;
- funzioni di coordinamento e supporto al CSIRT interno;
- attività di analisi specialistica e supporto avanzato.

Il Presidio opera **esclusivamente sugli strumenti messi a disposizione dall'Amministrazione**, quali, a titolo esemplificativo, piattaforme SIEM, SOAR, XDR, sistemi di ticketing e di gestione degli incidenti.

Il Fornitore **non fornisce né impone strumenti proprietari**, salvo diversa e specifica richiesta dell'Amministrazione.

Il Fornitore opera **a supporto delle funzioni dell'Amministrazione** responsabili della gestione degli incidenti di sicurezza informatica, inclusi il Punto di Contatto e il Referente CSIRT, **senza sostituirsi alle responsabilità normative che restano in capo all'Amministrazione**.

Nell'ambito del Presidio, il Fornitore può supportare l'Amministrazione nelle seguenti attività:

- presa in carico e analisi degli eventi e degli incidenti;
- triage e classificazione;
- supporto al contenimento, all'eradicazione e al ripristino;
- supporto alla predisposizione delle evidenze e della reportistica;
- supporto specialistico nella gestione di incidenti complessi o critici;
- trasferimento di competenze e affiancamento operativo al personale dell'Amministrazione.

Il Presidio non si configura come:

- servizio di monitoraggio autonomo del Fornitore;
- outsourcing completo della funzione di Incident Management;
- assunzione di responsabilità end-to-end sulla gestione degli incidenti;
- sostituzione delle strutture interne dell'Amministrazione.

2.2.1 Disposizioni generali del servizio

Le attività previste nel successivo paragrafo si svolgono nel rispetto delle seguenti disposizioni generali, applicabili trasversalmente a tutte le fasi del processo di gestione degli eventi e degli incidenti di sicurezza informatica.

1. Supporto alle attività di miglioramento continuo e alle *lesson learned*

Il Fornitore assiste l'Amministrazione Contraente nelle attività di miglioramento continuo del processo di gestione degli incidenti, incluse le analisi post-evento, la formalizzazione delle *lesson learned* e l'aggiornamento delle procedure operative interne. Tale supporto è assicurato per tutti i livelli del presidio, in funzione della severità dell'evento o dell'incidente e del contributo tecnico fornito. Nell'ambito delle attività di analisi post-evento e delle *lesson learned*, il Fornitore supporta l'Amministrazione nell'individuazione di eventuali mancate rilevazioni o ritardi di individuazione degli eventi di sicurezza (falsi negativi), contribuendo all'analisi delle cause e alla definizione di possibili azioni di miglioramento, fermo restando che la responsabilità delle capacità di detection resta in capo all'Amministrazione.

2. Supporto alle attività di segnalazione e agli adempimenti di notifica previsti dalla normativa nazionale ed europea

Nell'ambito delle rispettive competenze tecniche, il Fornitore collabora con l'Amministrazione nella predisposizione delle attività di segnalazione, pre-allarme e supporto alla notifica degli eventi e degli incidenti di sicurezza, in conformità alla normativa nazionale ed europea vigente, incluse le disposizioni emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN). Resta in capo all'Amministrazione la responsabilità ultima dell'invio delle comunicazioni verso ACN, CSIRT Italia o ulteriori autorità competenti.

3. Utilizzo di strumenti del Fornitore in assenza di strumenti equivalenti dell'Amministrazione

Qualora l'Amministrazione non disponga degli strumenti necessari per l'esecuzione di specifiche attività tecniche (ad esempio analisi di artefatti sospetti, reverse engineering, attività forensi specialistiche), il Fornitore potrà utilizzare strumenti propri, previa autorizzazione formale dell'Amministrazione. Tali strumenti dovranno operare esclusivamente su **copie** degli artefatti, in ambienti **isolati o stand-alone**, nel rispetto delle policy di sicurezza e delle regole di gestione delle evidenze digitali dell'Amministrazione.

2.2.2 Attività previste

Le attività di supporto afferenti ai servizi del presente ambito si articolano come segue e si basano sulla seguente **classificazione degli eventi e degli incidenti di sicurezza**.

Qualora l'Amministrazione Contraente adotti una classificazione degli eventi e degli incidenti di sicurezza diversa da quella indicata nel presente paragrafo, quanto previsto nei paragrafi del presente ambito dovrà essere adattato **alla classificazione adottata dall'Amministrazione**, nel rispetto dei propri modelli organizzativi e delle procedure interne.

La classificazione applicabile e le relative modalità operative dovranno essere **formalmente condivise e documentate nell'ambito del Piano di Lavoro Generale o di apposita documentazione concordata tra le parti**.

Tale documentazione **costituisce il riferimento operativo vincolante ai fini dell'erogazione del servizio e dell'esecuzione del Contratto Esecutivo**.

Severità	Descrizione
0 - HIGH	Incidenti ad alto impatto su continuità, dati, sicurezza nazionale; crisi cyber: - l'organizzazione non è più in grado di fornire uno o più servizi essenziali agli utenti; - dati/informazioni personali o proprietarie sono stati modificati, cancellati o esfiltrati; - il ripristino dall'incidente non è possibile (ad esempio, dati sensibili esfiltrati e diffusi, non recuperabili a seguito di un evento ransomware).
1 – MEDIUM	Incidenti ad impatto significativo, complessi, con necessità forense: - l'organizzazione è in grado di erogare un servizio essenziale solo ad una parte dell'utenza; - è stato rilevato l'accesso e l'esfiltrazione a dati/informazioni personali o proprietarie; - il ripristino è possibile con tempistiche non note in quanto, ad esempio, sono necessarie risorse aggiuntive o supporto esterno.
2- LOW	Incidenti confermati non critici: - l'organizzazione può ancora fornire tutti i servizi essenziali a tutti gli utenti, ma risultano non ottimali in termini di efficienza; - è stato rilevato l'accesso a dati/informazioni sensibili o proprietarie; - il ripristino è possibile con tempistiche note, anche tramite risorse aggiuntive.
3 – NONE	Eventi, anomalie, possibili falsi positivi: - nessun effetto sulla capacità dell'organizzazione di erogare i servizi agli utenti; - nessuna informazione è stata oggetto di accesso non autorizzato, esfiltrazione, modifica o cancellazione; - il tempo necessario per il ripristino è prevedibile con le risorse esistenti.

1. Rilevazione, analisi preliminare e classificazione degli eventi di sicurezza

Il Fornitore dovrà assicurare supporto sulle attività continuative di rilevazione, analisi preliminare e classificazione degli eventi di sicurezza informatica, mediante l'utilizzo esclusivo degli strumenti, delle piattaforme e delle evidenze rese disponibili dall'Amministrazione Contraente, nel rispetto delle procedure operative da questa definite. Inoltre, il Fornitore gestirà e chiuderà unicamente gli eventi a severità 3 – NONE, quali anomalie, segnalazioni non rilevanti, falsi positivi o situazioni che non configurano un incidente di sicurezza, mentre gli incidenti classificati dall'Amministrazione come **severità High, Medium o Low** devono essere **instradati ai livelli superiori** secondo le procedure dell'Amministrazione.

Le attività minime comprendono:

- **Supporto alle attività continuative di monitoraggio** degli eventi e delle segnalazioni generate dagli strumenti dell'Amministrazione, quali – a titolo esemplificativo – sistemi di monitoraggio e/o logging, eventuale SIEM, repository di segnalazioni, caselle di posta elettronica dedicate all'incident reporting, strumenti di ticketing o ulteriori asset organizzativi eventualmente presenti, secondo le modalità operative definite dalla stessa;
- **Analisi e Classificazione degli eventi**, mediante l'applicazione dei criteri di priorità e severità adottati dall'Amministrazione e comunque coerenti con le indicazioni emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN). In tale fase sono quindi identificati i falsi positivi e assegnato il livello di priorità agli incidenti in funzione delle regole definite dall'Amministrazione;
- **Apertura, aggiornamento e instradamento dei ticket**, o altro strumento previsto dall'Amministrazione, verso il successivo livello di analisi, secondo il modello di escalation definito dalla stessa;
- **Il Fornitore supporta la gestione e la chiusura degli eventi a severità 3 – NONE:**
 - o validazione del falso positivo;
 - o registrazione dell'anomalia;
 - o chiusura del ticket, o altro strumento, secondo le procedure dell'Amministrazione;
 - o eventuale segnalazione ricorrente da includere nel report periodico.
- **Produzione di report periodici**, con frequenza giornaliera o settimanale, in accordo con le esigenze rappresentate dall'Amministrazione;
- **Supporto alle attività operative di routine**, quali la gestione delle whitelist/blacklist, nei limiti e secondo le modalità definite dall'Amministrazione;
- **Collaborazione e costante allineamento con il personale dell'Amministrazione** o altro personale dalla stessa indicato.

Ulteriori attività richiedibili:

- Collaborazione, ove presenti, con Blue Team e/o Purple Team;

- Partecipazione a **simulazioni tabletop**, finalizzate alla validazione dei processi di gestione degli incidenti e delle procedure di escalation;
- Supporto al **tuning** delle regole di correlazione e detection degli strumenti SIEM dell'Amministrazione;
- Attività di **formazione operativa**, erogata nei limiti e con le modalità definite in sede di Piano di Lavoro Generale.

2. **Analisi avanzata, correlazione e supporto al contenimento dell'incidente**

Il Fornitore dovrà garantire, mediante personale qualificato, supporto nelle attività di analisi degli incidenti confermati che presentano un impatto limitato ma che richiedono attività di analisi approfondita, correlazioni multi-sorgente e definizione di misure di contenimento e ripristino secondo le procedure, i playbook e gli strumenti messi a disposizione dall'Amministrazione Contraente.

Le attività minime comprendono:

- **Analisi approfondita** degli eventi e degli alert instradati, mediante l'esame congiunto delle evidenze tecniche disponibili;
- **Correlazione degli eventi/evidenze** provenienti da fonti eterogenee, qualora presenti (es. sistemi SIEM, EDR/XDR, log applicativi, log di rete, telemetry di endpoint);
- Analisi e correlazione degli eventi e delle evidenze tecniche con informazioni di **threat intelligence disponibili**, quali indicatori di compromissione (IoC), tattiche, tecniche e procedure note, campagne di minaccia e contesto di rischio, ove disponibili;
- **Conferma e riclassificazione della severità**, ove necessario, sulla base delle evidenze raccolte;
- **Identificazione della causa primaria (root cause)** dell'incidente, mediante valutazione tecnica e ricostruzione della sequenza degli eventi;
- Identificazione degli **asset coinvolti** e valutazione **dell'impatto** tecnico, al fine di definire le misure di contenimento e ripristino;
- **Supporto alle attività di contenimento e ripristino**, in collaborazione con il personale dell'Amministrazione, secondo le procedure di response definite;
- **Gestione delle escalation** verso il livello superiore, nei casi in cui emergano elementi di complessità, persistenza, necessità forense o estensione dell'incidente;
- **Aggiornamento dei playbook** e delle regole operative e delle configurazioni di detection, ove richiesto dall'Amministrazione;
- **Predisposizione di report tecnici** di analisi e di chiusura dell'attività, secondo la periodicità e il formato definiti dall'amministrazione.

- **Ulteriori attività richiedibili** Attività di **threat hunting** di base;
- Partecipazione ad esercitazioni congiunte Blue/Purple Team;
- Partecipazione a **simulazioni tabletop** orientate agli scenari di incidenti;
- Supporto al **tuning delle regole SIEM/EDR**, nei limiti degli strumenti dell'Amministrazione.

3. Analisi specialistica, forense e supporto alla gestione degli incidenti complessi

Il Fornitore dovrà assicurare supporto nella gestione di incidenti complessi, ad alto impatto tecnico, che richiedono competenze specialistiche, acquisizione e analisi delle evidenze digitali e capacità tecniche di livello avanzato, come ad esempio:

- attività forense (endpoint, server, rete);
- analisi di minacce avanzate;
- investigazione su persistence, movimento laterale, esfiltrazione;
- misure di contenimento più complesse;
- primo livello di coordinamento interno con strutture dell'Amministrazione e CSIRT interni.

Le attività minime comprendono:

- **Analisi forense** su endpoint, server o apparati di rete, sulla base degli strumenti messi a disposizione dall'Amministrazione;
- **Threat hunting avanzato** e individuazione di eventuali indicatori di compromissione (IoC) o di attacco (IoA) non rilevati nei livelli precedenti;
- **Reverse engineering di file o artefatti sospetti**, nei limiti degli strumenti resi disponibili dall'Amministrazione, previa autorizzazione della stessa;
- **Valutazione avanzata dell'impatto**, inclusa ricostruzione della catena d'attacco;
- **Definizione delle misure di mitigazione**, raccomandazioni operative e individuazione di possibili misure correttive;
- **Supporto al contenimento avanzato** e alle decisioni operative dell'Amministrazione;
- **Escalation** se l'incidente evolve in un episodio ad alto impatto o con potenziali implicazioni istituzionali;
- **Produzione di report forensi e report tecnici avanzati**, secondo i contenuti e i formati stabiliti dall'Amministrazione;
- **Contributo** per la revisione dei playbook e per la definizione di misure preventive.
- **Ulteriori attività richiedibili:** Partecipazione ad esercitazioni **Red Team** e congiunte Blue/Purple Team;
- Contributo alle attività di analisi post-evento (lesson learned);
- Supporto alla definizione di strategie di hardening.

4. Gestione incidenti ad alto impatto, escalation critiche e coordinamento istituzionale

Il Fornitore dovrà garantire, mediante personale altamente qualificato, il supporto tecnico per la gestione degli incidenti di sicurezza informatica caratterizzati da elevata complessità, impatto significativo/sistemico o rilevanza istituzionale, secondo le modalità definite dall'Amministrazione Contraente.

Le attività minime comprendono:

- **Gestione dell'escalation tecnica** relativa a incidenti complessi, multilivello o multisorgente, che possano comportare impatti elevati sulla continuità operativa, sulla disponibilità dei servizi essenziali o sull'integrità dei dati;
- **Coordinamento tecnico con soggetti esterni**, quali CERT, CSIRT Italia, ACN, fornitori terzi o ulteriori autorità competenti, secondo le procedure e i canali definiti dall'Amministrazione;
- **Analisi forense avanzata**, nei limiti degli strumenti e delle risorse tecniche rese disponibili dall'Amministrazione, comprendente la raccolta, l'analisi e la valorizzazione di evidenze digitali a supporto delle attività di investigazione tecnica;
- **Supporto alla gestione della crisi cyber**, ove attivata dall'Amministrazione, mediante contributi tecnici utili alla definizione delle decisioni operative, alla gestione delle informazioni, alla comunicazione verso i livelli decisionali e all'integrazione con il processo di incident response;
- **Redazione di documentazione tecnica di alto livello** quali executive report, report forensi avanzati, dossier tecnici e note operative per autorità competenti, secondo i formati e le tempistiche stabilite dall'Amministrazione;
- **Contributo alla definizione delle strategie di ripristino e mitigazione**, sulla base delle evidenze tecniche emerse durante la gestione dell'incidente, anche ai fini della fase di "miglioramento continuo".
- **Ulteriori attività richiedibili: Partecipazione o supporto a esercitazioni di crisi su larga scala**, finalizzate a rafforzare la capacità di cooperazione interorganizzativa e la gestione degli scenari ad alto impatto;
- **Supporto tecnico alla revisione delle strategie di gestione degli incidenti ad alto impatto**, inclusa l'analisi delle lezioni apprese;
- **Sessioni di debriefing** a beneficio delle funzioni apicali dell'Amministrazione, finalizzate alla condivisione delle evidenze tecniche, dell'analisi degli impatti e delle opportunità di miglioramento **del processo di gestione degli incidenti**.

Il Fornitore dovrà condurre **SAL periodici settimanali** (o con diversa periodicità concordata con l'Amministrazione), e produrre la relativa documentazione in formato:

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

- **dettagliato** per le strutture operative;
- **executive** per le strutture direttive.

Inoltre, in caso di richieste di chiarimenti sull'operato da parte dell'Amministrazione, formalizzate attraverso i canali di comunicazione previsti o concordati nell'ambito del Contratto Esecutivo, il Fornitore dovrà fornire riscontro entro 2 giorni lavorativi.

2.2.3 Deliverable

Il presente capitolo descrive i deliverable minimi che il Fornitore dovrà produrre, suddivisi per ciascun livello operativo del servizio, in coerenza con le attività descritte nel paragrafo 2.2.2 **Attività previste**.

Tutti i deliverable dovranno:

- essere predisposti secondo i formati indicati dall'Amministrazione Contraente;
- essere trasmessi nei tempi e con le modalità stabilite nel Piano di Lavoro Generale;
- essere redatti in lingua italiana, salvo diversa indicazione dell'Amministrazione;
- essere conservati secondo quanto previsto dal modello di ticketing e di tracciamento adottato dall'Amministrazione;
- riferirsi esclusivamente agli strumenti, ai sistemi e alle evidenze rese disponibili dall'Amministrazione.

Il Fornitore dovrà produrre, almeno, i seguenti deliverable:

ID	TITOLO	DESCRIZIONE	SLA
IM_1	Registro eventi e attività	Registro cronologico a supporto delle attività di gestione degli eventi di sicurezza analizzati, delle attività di triage, delle classificazioni effettuate e delle eventuali escalation	Aggiornamento continuativo/giornaliero ; il registro costituisce base informativa per il Report periodico (IM_3) ed è reso disponibile all'Amministrazione su richiesta
IM_2	Ticket (o altra modalità indicata dall'Amministrazione) di gestione evento/incidente	Apertura, aggiornamento e chiusura dei ticket (o altra modalità indicata dall'Amministrazione) relativi a eventi e incidenti, con indicazione di severità, priorità, livello coinvolto e decisioni di escalation. <i>(Per tutte le attività)</i>	Contestuale alla gestione dell'evento/incidente secondo le procedure dell'Amministrazione.

ID	TITOLO	DESCRIZIONE	SLA
IM_3	Report periodico di rilevazione, analisi preliminare e classificazione degli eventi di sicurezza	Report operativo contenente: – volume degli eventi gestiti; – numero di falsi positivi identificati; – incidenti classificati per priorità/severità; – escalation verso livello successivo di analisi avanzata, correlazione e supporto al contenimento dell'incidente; – eventuali anomalie ricorrenti o pattern rilevati; – KPI e SLA per il livello; secondo i formati e le modalità indicate dall'Amministrazione.	Giornaliero o Settimanale o diversa tempistica indicata dall'Amministrazione
IM_4	Dashboard di monitoraggio eventi	Dashboard di monitoraggio e classificazione degli eventi (su strumenti dell'Amministrazione o stand-alone autorizzata), secondo i formati e le modalità indicate dall'Amministrazione.	Entro 10 giorni lavorativi dall'avvio del servizio; aggiornamento secondo periodicità concordata (es. giornaliera o settimanale).
IM_5	Report di analisi incidente	Report tecnico di analisi per incidenti di severità 2 (LOW), con evidenze raccolte, correlazioni, valutazione preliminare e azioni di contenimento suggerite ed eventualmente supportate. Il report, quindi, deve contenere almeno: – descrizione dell'evento e contesto di rilevazione; – perimetro analizzato e asset coinvolti; – fonti informative ed evidenze tecniche esaminate; – correlazioni effettuate tra eventi e log; – valutazione preliminare dell'impatto; – azioni di contenimento suggerite o supportate.	Entro 3 giorni lavorativi dalla chiusura tecnica dell'incidente, salvo diversa tempistica concordata.
IM_6	Root Cause Analysis (RCA)	Analisi strutturata della causa primaria dell'incidente e delle condizioni che ne hanno consentito il verificarsi, comprensiva degli impatti e delle possibili misure di mitigazione. La Root Cause Analysis deve includere almeno: – ricostruzione della sequenza degli eventi (timeline);	Entro 5 giorni lavorativi dalla chiusura dell'incidente, salvo diversa tempistica concordata.

ID	TITOLO	DESCRIZIONE	SLA
		– identificazione della causa primaria e dei fattori contributivi; – evidenze tecniche a supporto delle conclusioni; – indicazione delle misure correttive e preventive raccomandate.	
IM_7	Report forense	Report forense per incidenti complessi (severità 1 – MEDIUM) contenente almeno: – descrizione del perimetro analizzato; – evidenze digitali raccolte; – timeline tecnica dell'incidente; – analisi delle attività malevole rilevate; – eventuali indicatori di compromissione (IoC/IoA).	Entro 5 giorni lavorativi dalla conclusione delle attività forensi, salvo diversa tempistica concordata.
IM_8	Mitigation Plan tecnico	Documento con misure correttive, azioni di mitigazione e raccomandazioni operative a valle dell'incidente, incluse proposte di aggiornamento dei playbook di detection e response, ove richiesto dall'Amministrazione.	Entro 5 giorni lavorativi dalla consegna del report di riferimento.
IM_9	Executive technical note	Nota tecnica sintetica per i livelli direzionali dell'Amministrazione, relativa a incidenti complessi o ad alto impatto.	Entro 2 giorni lavorativi dalla richiesta dell'Amministrazione o dalla chiusura dell'incidente.
IM_10	Executive Report incidente critico	Report di sintesi per incidenti di severità 0 (HIGH), con descrizione dell'evento, impatti, decisioni e stato delle azioni. In particolare, il documento, destinato alle funzioni apicali dell'Amministrazione, contiene: – descrizione dell'incidente ad alto impatto; – sintesi delle attività condotte; – valutazione tecnica dell'impatto; – misure di contenimento adottate; – raccomandazioni strategiche.	Entro 2 giorni lavorativi dalla stabilizzazione dell'incidente.
IM_11	Report forense avanzato	Documento di analisi avanzata per incidenti critici, comprensivo di timeline estesa, analisi tecnica approfondita ed elementi a supporto delle attività di segnalazione e notifica istituzionale (L4).	Entro 3 giorni lavorativi dalla chiusura tecnica dell'incidente, salvo diversa tempistica concordata.

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

ID	TITOLO	DESCRIZIONE	SLA
IM_12	Documentazione di supporto alle notifiche	Documentazione tecnica a supporto delle attività di segnalazione, pre-allarme e notifica verso ACN, CSIRT o altre autorità competenti.	Entro i tempi richiesti dalla normativa applicabile, in coordinamento con l'Amministrazione.
IM_13	Lesson Learned	Documento di analisi post-evento con lezioni apprese e raccomandazioni di miglioramento del processo di incident management. Il documento di Lesson Learned deve includere, a titolo esemplificativo: – sintesi dell'incidente e delle criticità emerse; – gap di processo, tecnologici o organizzativi individuati; – raccomandazioni di miglioramento; – indicazione dei processi o playbook interessati.	Entro 10 giorni lavorativi dalla chiusura dell'incidente, salvo diversa tempistica concordata.
IM_14	SAL periodici	Stato Avanzamento Lavori del servizio, in formato operativo ed executive.	Settimanali , o con diversa periodicità concordata.
IM_15	Risposte a richieste di chiarimento	Riscontro alle richieste di chiarimento dell'Amministrazione sui deliverable o sulle attività svolte.	Entro 48 ore lavorative dalla richiesta dell'Amministrazione.

L'Amministrazione valuterà i deliverable entro **5 giorni lavorativi** dalla consegna. In caso di richieste di modifica, il Fornitore dovrà aggiornare/modificare i deliverable entro **5 giorni lavorativi** dalla comunicazione della PA, salvo diversa tempistica concordata.

Tutte le tempistiche dovranno essere indicate nel Piano di Lavoro Generale.

Gli adempimenti indicati nel presente paragrafo e ad esso collegati sono valutati ai fini di rilievi/penali in:

- 4.1 IQ01 – Rispetto di una scadenza contrattuale;
- 4.2 IQ02 – Adeguatezza delle figure professionali proposte per la erogazione dei servizi;
- 4.5 IQ05 - Turnover del personale impiegato nella fornitura;
- 4.6 IQ06 – Impegni assunti in offerta tecnica;
- 4.9 IQ09 – Tempestività di presa in carico del supporto di Incident Management;
- 4.10 IQ10 – Qualità del triage e della classificazione degli eventi;
- 4.11 IQ11 – Conformità del supporto alle procedure dell'Amministrazione;
- 4.12 IQ12 – Efficacia del supporto specialistico senza ulteriore escalation;

- 4.13 IQ13 – Completezza delle evidenze tecniche per decisioni e notifiche;
- 4.22 IQ22 – Rilievi su obbligazioni contrattuali non presidiate.

2.2.4 Figure professionali coinvolte

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 al capitolo 3 *Risorse da impiegare nell'esecuzione dei servizi*):

1. Security Principal
2. Forensics Expert
3. Security Analyst
4. Security Specialist
5. Incident Responder
6. Information Security Manager
7. Security Engineer
8. Network Security Engineer

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

2.2.5 Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento di tutti i servizi è: **Giorno/Persona**.

La modalità di remunerazione di tutti i servizi è: **a tempo/spesa oppure a corpo**.

In fase di offerta è richiesto al Concorrente di esprimere un prezzo per giorno/persona per ogni figura professionale prevista. I prezzi espressi saranno riferiti rispettivamente a:

- 8 ore lavorative complessive nella fascia oraria ferial Lun-Sab 8.00-20.00 (fascia standard);
- 8 ore lavorative complessive nella fascia oraria Lun-Sab 20.00-7.00 o la domenica o nei giorni festivi (fascia straordinaria).

In sede di Piano dei fabbisogni, l'Amministrazione definirà i deliverables richiesti e le risorse necessarie, indicando quindi il mix necessario per le attività richieste, in un'ottica di coerenza e proporzionalità.

2.3 Continuous Vulnerability Management

Il **Continuous Vulnerability Management (CVM)** è un **ambito funzionale** finalizzato a supportare l'Amministrazione nel **governo continuo della superficie di attacco e della postura di sicurezza**,

attraverso un insieme coordinato di servizi tecnici e specialistici orientati all'identificazione, alla valutazione e alla gestione del rischio derivante dalle vulnerabilità di sicurezza.

L'ambito CVM comprende **servizi distinti e complementari**, tra cui attività di vulnerability assessment, penetration test, red teaming, blue teaming, purple teaming, analisi e integrazione delle evidenze di rischio e valutazione periodica della postura di sicurezza dell'Amministrazione e, ove previsto, dei fornitori.

I servizi attivabili al presente ambito sono progettati per fornire all'Amministrazione una **visione strutturata, contestualizzata e progressiva del rischio**, supportando i processi decisionali in materia di prioritizzazione degli interventi di sicurezza e di miglioramento continuo della postura di sicurezza, **senza configurarsi come servizi gestiti né come sostituzione delle responsabilità di governo**, che restano in capo all'Amministrazione.

I servizi del CVM si integrano con gli altri ambiti del Capitolato (in particolare Asset Inventory, Incident Management e Sicurezza dei sistemi e delle applicazioni), **in un'ottica di complementarità e coerenza**, fermo restando che ciascun servizio mantiene il proprio perimetro funzionale e operativo come descritto nei paragrafi successivi.

Le attività afferenti al presente ambito sono orientate alla valutazione e al miglioramento della postura di sicurezza e non comportano la presa in carico operativa di eventi o incidenti di sicurezza, che restano disciplinati dall'ambito di Incident Management.

2.3.1 Attività previste

Nell'ambito delle attività di Vulnerability Assessment, Penetration Test e analisi avanzata della postura di sicurezza, il Fornitore supporta l'Amministrazione anche nella valutazione degli asset applicativi e dei servizi che utilizzano o integrano tecnologie di Intelligenza Artificiale e Machine Learning, con riferimento ai rischi specifici dei modelli, delle pipeline, delle API e dei dataset utilizzati.

1. Vulnerability Assessment

Il servizio di **Vulnerability Assessment** supporta l'Amministrazione nell'esecuzione continuativa e strutturata delle attività di individuazione e analisi delle vulnerabilità di sicurezza presenti sugli asset infrastrutturali, applicativi e, ove presenti, OT/IoT.

Il Fornitore assiste l'Amministrazione nella **definizione dello scope** delle attività, individuando gli asset da sottoporre ad analisi in coerenza con l'Asset Inventory, con la criticità dei servizi e con le priorità di rischio definite dall'Amministrazione stessa. Il servizio si integra con l'Asset Inventory e con i processi di Risk Management adottati dall'Amministrazione, al fine di garantire una corretta contestualizzazione delle vulnerabilità rispetto alla criticità degli asset e dei servizi.

Il supporto comprende la configurazione e la schedulazione delle scansioni di vulnerabilità, utilizzando gli strumenti disponibili presso l'Amministrazione (a titolo esemplificativo: Qualys, Nessus, Tenable, OpenVAS), nonché l'analisi tecnica dei risultati prodotti.

Una componente centrale del servizio è rappresentata dalla **validazione dei risultati**, con particolare attenzione:

- all'identificazione e riduzione dei falsi positivi;
- alla corretta classificazione delle vulnerabilità;
- alla prioritizzazione delle vulnerabilità che tenga conto non solo della severità tecnica (CVSS), ma anche della reale esposizione degli asset e dell'impatto sui servizi e sui processi dell'Amministrazione e delle metodologie di gestione del rischio della stessa.

Il Fornitore supporta l'Amministrazione nella redazione di **report tecnici dettagliati**, comprensivi di raccomandazioni di remediation, nonché nella verifica dell'efficacia delle azioni correttive tramite attività di rescan.

Le attività sono pianificate su base periodica o continuativa, al fine di garantire il mantenimento nel tempo della postura di sicurezza.

2. Penetration Test

Il servizio di **Penetration Test** fornisce supporto specialistico per la simulazione controllata di attacchi informatici, finalizzati a valutare l'effettiva sfruttabilità delle vulnerabilità e l'impatto reale sugli asset e sui servizi dell'Amministrazione.

Il Fornitore assiste l'Amministrazione nella definizione dello **scope e delle regole di ingaggio** in funzione degli obiettivi dell'assessment, includendo:

- **Black Box:** il Penetration Test è condotto **senza fornire informazioni preliminari** al Fornitore in merito all'architettura, alle configurazioni o alle credenziali dei sistemi oggetto di test, simulando il comportamento di un attaccante esterno privo di conoscenza del contesto interno.
- **Grey Box:** il Penetration Test è condotto fornendo al Fornitore **un insieme limitato e controllato di informazioni**, quali ad esempio documentazione architeturale di alto livello, account con privilegi limitati o informazioni parziali sugli asset, al fine di simulare scenari di attacco più realistici e mirati.
- **White Box:** il Penetration Test è condotto fornendo al Fornitore **informazioni complete** sul perimetro oggetto di test, incluse architetture, configurazioni, codice sorgente e credenziali, al fine di valutare in modo approfondito la postura di sicurezza e individuare vulnerabilità difficilmente rilevabili con approcci meno informati.

Le attività comprendono fasi di raccolta informazioni, analisi delle vulnerabilità mediante strumenti automatici e tecniche manuali, nonché attività di **exploitation controllata** volte a dimostrare l'impatto concreto delle debolezze individuate.

Le attività di Penetration Test possono essere pianificate e condotte anche a partire dai risultati dei Vulnerability Assessment precedentemente eseguiti, utilizzando tali evidenze come input per orientare e rendere più mirate le attività di test, con particolare riferimento alle vulnerabilità ad elevato impatto, ai sistemi critici e agli scenari di rischio ritenuti prioritari dall'Amministrazione.

Ove richiesto, il servizio può includere attività di **post-exploitation**, quali escalation dei privilegi, movimento laterale e simulazioni di esfiltrazione dei dati, sempre nel rispetto delle regole di ingaggio concordate.

Il servizio si conclude con un **debriefing tecnico** e la produzione di un **report dettagliato**, corredato da un executive summary per i livelli decisionali, nonché con il supporto alla remediation e alla verifica post-intervento.

3. Analisi e integrazione dei risultati da fonti eterogenee

L'obiettivo del servizio non è la mera individuazione puntuale delle vulnerabilità, bensì il **miglioramento progressivo e misurabile della postura di sicurezza**, attraverso:

- una visione integrata delle debolezze tecniche;
- la contestualizzazione del rischio rispetto agli asset, ai servizi e alle minacce attive;
- il supporto alle decisioni dell'Amministrazione in materia di prioritizzazione e trattamento del rischio.

Il servizio valorizza anche le evidenze provenienti dai processi di gestione degli incidenti di sicurezza, al fine di supportare l'analisi delle cause ricorrenti, l'individuazione di eventuali gap di detection e il miglioramento complessivo della postura di sicurezza.

Il servizio rappresenta altresì un livello di integrazione e valorizzazione delle evidenze prodotte dalle attività di assessment e testing, ed è finalizzato a supportare l'Amministrazione nella lettura complessiva del rischio.

Questo servizio consente all'Amministrazione di superare una visione frammentata delle vulnerabilità, fornendo un **quadro integrato del rischio** attraverso la correlazione di evidenze provenienti da fonti eterogenee.

Il Fornitore supporta la raccolta, la normalizzazione e il consolidamento dei dati provenienti, a titolo esemplificativo, da:

- Vulnerability Assessment e Penetration Test;

- Analisi del codice (SAST/DAST/MAST);
- Processi di Risk Management;
- Threat intelligence;
- Audit e questionari di sicurezza.

Le informazioni vengono correlate al fine di mettere in relazione le vulnerabilità tecniche con:

- minacce attive e campagne note;
- criticità degli asset e dei servizi;
- impatti di business.

Il risultato è una **prioritizzazione del rischio basata su contesto reale e le metodologie dell'Amministrazione**, supportata da report integrati e dashboard di sintesi, utili alla definizione dei piani di remediation e alle attività di follow-up.

Le attività di identificazione, analisi, prioritizzazione e trattamento delle vulnerabilità sono svolte **nel rispetto della metodologia di Risk Management adottata dall'Amministrazione**, cui il Fornitore si allinea, operando a supporto dei processi decisionali e senza introdurre metodologie alternative non concordate.

4. Valutazione periodica della postura di sicurezza dell'Amministrazione e dei fornitori

Il servizio supporta l'Amministrazione nella valutazione periodica della **postura di sicurezza complessiva**, includendo fornitori critici e supply chain.

Il Fornitore assiste l'Amministrazione nella definizione del perimetro di valutazione e nella raccolta delle informazioni tramite:

- **questionari e interviste**, finalizzati a raccogliere informazioni strutturate su processi, controlli di sicurezza, asset e pratiche operative, anche in relazione ai fornitori e alla supply chain;
- **analisi OSINT (Open Source Intelligence)**, svolta mediante l'analisi di fonti pubbliche e aperte, senza accesso a sistemi interni, al fine di valutare la visibilità esterna degli asset, dei servizi e delle informazioni dell'Amministrazione e dei soggetti terzi;
- **scansioni esterne**, volte a identificare configurazioni esposte, servizi pubblicamente accessibili e potenziali vulnerabilità rilevabili dall'esterno;
- **strumenti di security rating**, ove adottati, utilizzati come ulteriore elemento informativo per la valutazione comparativa della postura di sicurezza e del rischio associato a fornitori e terze parti.

Le attività consentono di:

- valutare il livello di maturità della sicurezza;

- individuare gap rispetto a standard e best practice;
- supportare processi di vendor risk management e due diligence;
- rafforzare la compliance normativa.

Il servizio include il supporto al follow-up delle azioni correttive e l'integrazione con i processi di audit e di gestione dei fornitori.

5. Red Team

Il servizio di **Red Team** è finalizzato alla **simulazione di campagne di attacco avanzate e realistiche**, ispirate a minacce effettivamente osservate nel panorama cyber, con l'obiettivo di valutare la **resilienza complessiva dell'Amministrazione** rispetto ad attacchi complessi e mirati.

Le attività di Red Team sono **pianificate congiuntamente con l'Amministrazione**, attraverso:

- la definizione degli **obiettivi** del test (ad esempio: compromissione di un servizio critico, accesso non autorizzato a dati sensibili, interruzione di un processo);
- la costruzione di **scenari di attacco realistici**, coerenti con il contesto operativo e tecnologico della PA;
- la definizione delle **regole di ingaggio (Rules of Engagement)**, che stabiliscono perimetro, limiti operativi, tecniche consentite, finestre temporali e modalità di conduzione delle attività.

Le simulazioni di attacco si basano sull'utilizzo di **TTP (Tactics, Techniques and Procedures)** riconducibili a framework di riferimento riconosciuti a livello internazionale, quali **MITRE ATT&CK**, al fine di garantire che le attività riproducano comportamenti di attaccanti reali e non semplici test teorici o automatizzati.

Il servizio di Red Team consente di valutare non solo la presenza di vulnerabilità tecniche, ma anche:

- la capacità dell'organizzazione di **rilevare** attività malevole;
- l'efficacia delle misure di **contenimento**;
- la prontezza e l'adeguatezza della **risposta ad attacchi complessi**, inclusi scenari multi-vettore o persistenti.

6. Blue Team

Il servizio di **Blue Team** supporta le funzioni difensive dell'Amministrazione nelle attività di **monitoraggio, rilevazione e risposta agli eventi e agli incidenti di sicurezza**, contribuendo al miglioramento continuo delle capacità operative.

Il Fornitore affianca il personale dell'Amministrazione nelle attività di:

- analisi e correlazione degli eventi di sicurezza generati dagli strumenti di monitoraggio (SIEM, EDR/XDR, IDS/IPS);
- **threat hunting proattivo**, volto all'individuazione di minacce avanzate o persistenti non immediatamente rilevate dai controlli automatici;
- gestione degli incidenti, incluse le fasi di triage, analisi, contenimento, supporto all'eradicazione e attività post-evento;
- **tuning e aggiornamento delle regole di detection** e dei casi d'uso di sicurezza;
- sviluppo, aggiornamento e verifica dei **playbook di risposta agli incidenti**, in coerenza con i processi dell'Amministrazione.

Il servizio include inoltre:

- attività di **reporting periodico** sugli eventi, sugli incidenti e sui trend osservati;
- supporto alle attività di **compliance normativa** (ad es. NIS2, ISO/IEC 27001, GDPR);
- **formazione operativa e simulazioni tabletop**, finalizzate a rafforzare la preparazione del personale dell'Amministrazione nella gestione di scenari di incidente.

7. Purple Team

Il servizio di **Purple Team** è configurato come **supporto tecnico-specialistico alle strutture dell'Amministrazione** coinvolte nelle attività di sicurezza informatica ed è finalizzato a favorire il **coordinamento operativo e il miglioramento continuo** tra le funzioni di attacco simulato (Red Team) e le funzioni difensive e di risposta (Blue Team).

Il servizio non si configura come una funzione autonoma o esternalizzata, ma opera **in affiancamento al personale dell'Amministrazione**, integrandosi con i processi, gli strumenti e i modelli organizzativi già in essere, al fine di trasformare le evidenze emerse dalle attività di test e di difesa in **azioni concrete di rafforzamento delle capacità di detection, risposta e resilienza**.

Le sessioni di Purple Team prevedono la **collaborazione diretta** tra attività offensive e difensive, consentendo di:

- eseguire simulazioni di attacco (Red Team) in **tempo controllato**;
- osservare e analizzare in tempo reale la capacità di rilevazione e risposta del Blue Team;
- individuare **gap di detection, logging, correlazione ed escalation**;
- aggiornare e ottimizzare le regole SIEM/SOAR e i playbook di risposta;
- tradurre le evidenze tecniche emerse in **azioni di miglioramento concreto** dei processi e dei controlli di sicurezza.

Il servizio di Purple Team favorisce la condivisione delle conoscenze, la formalizzazione delle **lesson learned** e l'allineamento tra le diverse funzioni coinvolte nella sicurezza, riducendo il divario tra test offensivi e capacità difensive operative.

Per tutte le attività gestite dal Fornitore nell'ambito del presente paragrafo, lo stesso dovrà condurre **SAL periodici settimanali** (o con diversa periodicità concordata con l'Amministrazione), e produrre la relativa documentazione in formato:

- **dettagliato** per le strutture operative;
- **executive** per le strutture direttive.

Inoltre, in caso di richieste di chiarimenti sull'operato da parte dell'Amministrazione, formalizzate attraverso i canali di comunicazione previsti o concordati nell'ambito del Contratto Esecutivo, il Fornitore dovrà fornire riscontro entro 2 giorni lavorativi.

2.3.2 Deliverable

Il presente paragrafo descrive i **deliverable minimi** che il Fornitore dovrà produrre nell'ambito del servizio di Continuous Vulnerability Management, in coerenza con le attività descritte nel presente capitolo e con quanto definito nel Piano di Lavoro Generale e nei singoli Contratti Esecutivi.

I deliverable sono finalizzati a supportare l'Amministrazione nelle attività di governance, valutazione del rischio, prioritizzazione degli interventi e miglioramento continuo della postura di sicurezza.

ID	TITOLO	DESCRIZIONE	SLA
CVM_1	Registro delle vulnerabilità	Registro strutturato delle vulnerabilità identificate sugli asset dell'Amministrazione, comprensivo di severità, CVSS, asset coinvolti, stato, data rilevazione e riferimenti alle evidenze. Il registro è mantenuto aggiornato utilizzando gli strumenti dell'Amministrazione o formati concordati.	Aggiornamento continuativo / periodico secondo Piano di Lavoro concordato con l'Amministrazione
CVM_2	Report di Vulnerability Assessment	Report tecnico dettagliato delle attività di Vulnerability Assessment svolte, comprensivo di metodologia adottata, scope, risultati, validazione	Entro 10 giorni lavorativi dalla conclusione delle attività di Vulnerability Assessment, salvo

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

ID	TITOLO	DESCRIZIONE	SLA
		dei falsi positivi, classificazione e raccomandazioni di remediation. Il report è fornito utilizzando formati concordati con l'Amministrazione	diversa tempistica concordata con l'Amministrazione nel Piano di Lavoro Generale.
CVM_3	Dashboard vulnerabilità	Dashboard di monitoraggio delle vulnerabilità e della postura di esposizione, realizzata su strumenti dell'Amministrazione o in formato stand-alone autorizzato, con indicatori di severità, trend e copertura.	Entro 5 giorni lavorativi dalla consegna del report. La dashboard è aggiornata in itinere , con periodicità concordata nel Piano di Lavoro Generale, sulla base delle attività di Vulnerability Assessment, Penetration Test e delle ulteriori evidenze rese disponibili dall'Amministrazione.
CVM_4	Report di Penetration Test	Report tecnico del Penetration Test, comprensivo di scope, regole di ingaggio, percorsi critici e vulnerabilità sfruttate, impatti, evidenze, raccomandazioni tecniche e executive summary per i livelli decisionali.	Entro 15 giorni lavorativi dalla conclusione delle attività di Penetration Test, salvo diversa tempistica concordata con l'Amministrazione nel Piano di Lavoro Generale.
CVM_5	Report integrato di rischio	Report di integrazione e correlazione delle evidenze provenienti da VA, PT, analisi del codice, threat intelligence e altre fonti, finalizzato alla prioritizzazione del rischio in base al contesto operativo dell'Amministrazione. La prioritizzazione del rischio e la definizione delle raccomandazioni sono effettuate in coerenza con la metodologia di gestione del rischio dell'Amministrazione, tenendo conto delle classificazioni, delle soglie e dei criteri dalla stessa adottati.	Entro 10 giorni lavorativi dalla disponibilità completa delle evidenze di input (VA, PT, analisi del codice, threat intelligence), salvo diversa tempistica concordata. Il report può essere aggiornato in itinere , su richiesta dell'Amministrazione o al verificarsi di variazioni significative del contesto di rischio, secondo le modalità e le

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

ID	TITOLO	DESCRIZIONE	SLA
			tempistiche definite nel Piano di Lavoro Generale.
CVM_6	Valutazione postura Amministrazione e fornitori	Report periodico di valutazione della postura di sicurezza dell'Amministrazione e, ove previsto, dei fornitori critici, comprensivo di scoring, gap analysis e raccomandazioni di miglioramento.	Con periodicità trimestrale , oppure entro 15 giorni lavorativi dalla richiesta dell'Amministrazione per valutazioni ad evento.
CVM_7	Report Red Team	Documentazione tecnica delle attività di Red Team, comprensiva di scenari simulati, TTP utilizzate, evidenze raccolte, impatti e raccomandazioni di miglioramento.	Entro 15 giorni lavorativi dalla conclusione delle attività di Red Team, salvo diversa tempistica concordata.
CVM_8	Report Blue Team	Report delle attività di supporto Blue Team, comprensivo di analisi eventi, threat hunting svolto, tuning effettuati e raccomandazioni operative.	Con periodicità mensile , oppure secondo quanto definito nel Piano di Lavoro Generale.
CVM_9	Report Purple Team / Lesson Learned	Report di sintesi delle sessioni Purple Team, comprensivo di gap individuati, aggiornamenti a regole e playbook e lesson learned condivise con l'Amministrazione.	Entro 10 giorni lavorativi dalla conclusione della sessione Purple Team.
CVM_10	Mitigation & Remediation Plan	Documento di supporto alla definizione delle azioni correttive e di mitigazione a valle delle attività di Vulnerability Assessment, Penetration Test, analisi integrata del rischio, Red Team, Purple Team e valutazione della postura di sicurezza. Il documento include la prioritizzazione degli interventi, le dipendenze tecniche e organizzative e le raccomandazioni operative, senza assunzione di responsabilità esecutiva, che resta in capo all'Amministrazione.	Entro 10 giorni lavorativi dalla richiesta dell'Amministrazione o dalla consegna del report di riferimento.
CVM_11	SAL periodici	Stato Avanzamento Lavori del servizio, in formato operativo ed executive, con riepilogo attività svolte, criticità e azioni pianificate.	Settimanale / mensile oppure con diversa periodicità concordata con

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

ID	TITOLO	DESCRIZIONE	SLA
			l'Amministrazione e indicata nel Piano di Lavoro Geberale
CVM_12	Risposte a richieste di chiarimento	Riscontri tecnici a richieste di chiarimento dell'Amministrazione su attività o deliverable prodotti.	Entro 48 ore lavorative

L'Amministrazione valuterà i deliverable entro **5 giorni lavorativi** dalla consegna. In caso di richieste di modifica, il Fornitore dovrà aggiornare/modificare i deliverable entro **5 giorni lavorativi** dalla comunicazione della PA, salvo diversa tempistica concordata.

Tutte le tempistiche dovranno essere indicate nel Piano di Lavoro Generale.

Gli adempimenti indicati nel presente paragrafo e ad esso collegati sono valutati ai fini di rilievi/penali in:

- 4.1 IQ01 – *Rispetto di una scadenza contrattuale;*
- 4.2 IQ02 – *Adeguatezza delle figure professionali proposte per la erogazione dei servizi;*
- 4.5 IQ05 - *Turnover del personale impiegato nella fornitura;*
- 4.6 IQ06 – *Impegni assunti in offerta tecnica;*
- 4.13 IQ13 – *Completezza delle evidenze tecniche per decisioni e notifiche;*
- 4.22 IQ22 – *Rilievi su obbligazioni contrattuali non presidiate.*

2.3.3 Figure professionali coinvolte

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 al capitolo 3 *Risorse da impiegare nell'esecuzione dei servizi*):

- Security Principal;
- Cloud Security Expert;
- Senior Security Consultant;
- Security Analyst;
- Security Specialist;
- Junior Security Consultant;
- Threat intelligence specialist;
- Incident responder;
- Information Security Manager;
- Senior Penetration Tester;

- Junior Penetration Tester.

Con riferimento ad attività di Continuous Vulnerability Management che coinvolgano componenti o servizi basati su tecnologie di Intelligenza Artificiale e Machine Learning, il Fornitore **può avvalersi**, ove necessario, anche della figura professionale specialistica:

- AI Security Specialist.

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

2.3.4 Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento di tutti i servizi è: **Giorno/Persona**.

La modalità di remunerazione di tutti i servizi è: **a tempo/spesa oppure a corpo**.

In fase di offerta è richiesto al Concorrente di esprimere un prezzo per giorno/persona per ogni figura professionale prevista. I prezzi espressi saranno riferiti rispettivamente a:

- 8 ore lavorative complessive nella fascia oraria feriali Lun-Sab 8.00-20.00 (fascia standard);
- 8 ore lavorative complessive nella fascia oraria Lun-Sab 20.00-7.00 o la domenica o nei giorni festivi (fascia straordinaria).

In sede di Piano dei fabbisogni, l'Amministrazione definirà i deliverables richiesti e le risorse necessarie, indicando quindi il mix necessario per le attività richieste, in un'ottica di coerenza e proporzionalità.

2.4 Sicurezza dei sistemi e delle applicazioni

Il presente capitolo disciplina l'**ambito** dei servizi di **sicurezza dei sistemi e delle applicazioni** erogati mediante l'impiego di **personale specializzato del Fornitore**, che opera **direttamente sull'infrastruttura tecnologica dell'Amministrazione**, nel rispetto delle **metodologie operative, dei processi organizzativi e delle regole di governo della sicurezza adottate dall'Amministrazione stessa**.

Le attività sono svolte in coordinamento con le strutture tecniche dell'Amministrazione e secondo i processi di gestione già in uso (quali, a titolo esemplificativo, change management, configuration management, incident management e vulnerability management), garantendo la piena **integrazione operativa** del personale del Fornitore nei flussi di lavoro dell'Amministrazione e la **continuità dei servizi istituzionali**.

Il personale del Fornitore utilizza prioritariamente **gli strumenti, le piattaforme e le soluzioni tecnologiche già disponibili presso l'Amministrazione**. L'eventuale impiego di **strumenti propri del Fornitore** è consentito **esclusivamente ove necessario, previa autorizzazione formale dell'Amministrazione** e **senza oneri aggiuntivi** per la stessa, nel rispetto delle policy di sicurezza, dei vincoli di compliance e delle regole di trattamento dei dati vigenti.

I servizi descritti nel presente capitolo sono finalizzati a **ridurre la superficie di attacco, prevenire e individuare vulnerabilità, rafforzare la postura di sicurezza applicativa e infrastrutturale e supportare l'adozione dei principi di security by design e security by default**, in coerenza con le Linee guida AgID, con i principali standard internazionali di riferimento e con quanto già previsto negli altri ambiti del capitolato.

Nell'ambito della presente iniziativa, le attività di **hardening e patching** sono riferite esclusivamente **alle soluzioni e ai sistemi di sicurezza** adottati dall'Amministrazione (a titolo esemplificativo: soluzioni di sicurezza perimetrale, di protezione degli endpoint e dei server, di gestione degli accessi, di monitoraggio e rilevazione degli eventi di sicurezza).

Restano pertanto **escluse** dal perimetro del servizio le attività di hardening e patching riferite ai sistemi informativi, applicativi o infrastrutturali dell'Amministrazione **non riconducibili a soluzioni di sicurezza**, che sono disciplinate nell'ambito di altre iniziative o contratti di diversa natura.

2.4.1 Attività previste

1. Static Application Security Testing (SAST)

Descrizione del servizio

Il servizio di **Static Application Security Testing (SAST)** è un **servizio professionale di sicurezza applicativa** finalizzato all'identificazione delle vulnerabilità di sicurezza presenti nel codice delle applicazioni dell'Amministrazione, mediante tecniche di analisi statica condotte sul codice sorgente o binario, senza necessità di esecuzione dell'applicazione.

Il servizio è erogato da **personale specializzato del Fornitore**, che opera **nell'ambito dell'infrastruttura applicativa e dei processi di sviluppo dell'Amministrazione**, secondo le **metodologie, le procedure e le regole operative adottate dall'Amministrazione**.

L'attività è orientata a supportare l'Amministrazione nell'individuazione e nella correzione delle vulnerabilità nelle **fasi iniziali del ciclo di vita del software**, riducendo il rischio che difetti strutturali vengano propagati negli ambienti di test o di produzione e favorendo l'adozione dei principi di **security by design e secure-by-default**.

Ambito di applicazione

Il perimetro del servizio comprende l'analisi statica del codice delle seguenti categorie applicative dell'Amministrazione:

- applicazioni sviluppate ad hoc, sia internamente sia tramite fornitori esterni;
- componenti software open source utilizzati all'interno delle applicazioni;
- librerie e framework di terze parti;
- moduli applicativi integrati in sistemi informativi più ampi.

Ai fini del servizio, il termine *applicazione* è inteso come l'insieme di componenti software, sviluppate in linguaggi e framework differenti, finalizzate a soddisfare specifiche esigenze funzionali dell'Amministrazione.

Modalità di esecuzione del servizio

Il servizio è svolto dal Fornitore **in coordinamento con le strutture tecniche dell'Amministrazione** e prevede, almeno, le seguenti attività:

- definizione congiunta del perimetro di analisi in termini di applicazioni, moduli, linguaggi e tecnologie oggetto di verifica;
- utilizzo prioritario degli **strumenti di analisi statica già in uso presso l'Amministrazione**, ove disponibili e idonei allo scopo;
- configurazione ed esecuzione delle analisi statiche sul codice sorgente o binario;
- validazione dei risultati al fine di individuare e ridurre i falsi positivi;
- classificazione delle vulnerabilità secondo standard di settore condivisi;
- supporto tecnico all'Amministrazione e ai team di sviluppo per la comprensione delle vulnerabilità rilevate;
- verifica dell'efficacia delle azioni correttive adottate (re-testing), ove richiesto.

L'eventuale utilizzo di **strumenti o soluzioni del Fornitore** è consentito **esclusivamente previo accordo con l'Amministrazione, in assenza di strumenti equivalenti già disponibili e senza oneri aggiuntivi** per la Amministrazione.

Tipologie di controlli di sicurezza

L'attività di analisi statica del codice è svolta secondo le best practice internazionali e comprende, almeno, i seguenti ambiti di controllo:

- **Data Validation:** verifica delle modalità di gestione dei dati in ingresso, al fine di individuare vulnerabilità legate a input non validati o malformati che possano determinare comportamenti anomali dell'applicazione;
- **Control Flow:** analisi dei flussi di esecuzione del codice per individuare sequenze operative non sicure che possano generare violazioni di memoria, condizioni di errore o utilizzi impropri di componenti applicative;
- **Analisi semantica:** individuazione di problematiche legate all'uso non corretto di funzioni, metodi o API, incluse funzioni deprecate o intrinsecamente insicure;
- **Configurazioni applicative:** verifica dei parametri di configurazione dell'applicazione che possano introdurre debolezze di sicurezza;
- **Buffer Validation:** rilevazione di condizioni di buffer overflow o di letture/scritture oltre i limiti previsti.

Il servizio consente l'individuazione di vulnerabilità critiche quali, a titolo esemplificativo e non esaustivo: **SQL Injection, Cross-Site Scripting (XSS), buffer overflow, gestione non sicura degli errori, back-door logiche e vulnerabilità derivanti da dipendenze software.**

Standard e riferimenti metodologici

Le attività di SAST sono svolte dal Fornitore in coerenza con:

- OWASP Top 10;
- tassonomie e classificazioni di settore (CVE, CVSS, CWE);
- metodologie di sicurezza applicativa riconosciute a livello internazionale;
- **Linee Guida AgID per lo sviluppo del software sicuro nella Pubblica Amministrazione**, incluse le indicazioni su secure coding e sicurezza by design.

Integrazione nei processi dell'Amministrazione

Ove previsto dall'Amministrazione, il servizio può essere integrato nei **processi di sviluppo, manutenzione e rilascio del software già adottati dalla PA**, inclusi contesti DevSecOps, al fine di:

- rendere strutturali le verifiche di sicurezza sul codice;
- fornire feedback tempestivi ai team di sviluppo;
- supportare il miglioramento continuo della qualità e della sicurezza del software.

Il servizio è erogato dal Fornitore mediante l'impiego di **risorse professionali con competenze specialistiche in sicurezza applicativa**, operanti secondo i processi e gli strumenti dell'Amministrazione e, in caso siano utilizzati strumenti propri, come prima indicato, **senza oneri aggiuntivi** per la stessa.

2. Dynamic Application Security Testing (DAST)

Descrizione del servizio

Il servizio di **Dynamic Application Security Testing (DAST)** è un servizio professionale di sicurezza applicativa finalizzato all'identificazione delle vulnerabilità di sicurezza sfruttabili in fase di esecuzione all'interno delle applicazioni dell'Amministrazione, incluse applicazioni **web**, **servizi API (REST/SOAP)** ed eventuali componenti mobile backend, mediante tecniche di analisi dinamica.

Il servizio è erogato da **personale specializzato del Fornitore**, che opera **sull'infrastruttura applicativa dell'Amministrazione** e nel rispetto delle **metodologie, dei processi di sviluppo e delle regole operative adottate dalla stessa**.

L'attività è svolta secondo un approccio di **black-box testing**, basato sull'analisi dei comportamenti dell'applicazione in risposta a input controllati, al fine di valutare l'effettiva esposizione al rischio di attacchi informatici in condizioni di runtime.

Ambito di applicazione

Il perimetro del servizio comprende l'analisi dinamica delle seguenti tipologie di applicazioni e componenti dell'Amministrazione:

- applicazioni web accessibili tramite browser;
- servizi applicativi esposti tramite **API REST e servizi SOAP**;
- web service e interfacce applicative utilizzate da sistemi terzi o applicazioni legacy;
- componenti applicativi integrati in architetture più ampie.

Ai fini del servizio, l'analisi è focalizzata sulle funzionalità effettivamente esposte in esecuzione e sulle modalità di interazione dell'applicazione con utenti, sistemi e servizi esterni.

Modalità di esecuzione del servizio

Il servizio è svolto dal Fornitore **in coordinamento con le strutture tecniche dell'Amministrazione** e prevede, almeno, le seguenti attività:

- definizione congiunta del perimetro di analisi in termini di applicazioni, endpoint, funzionalità e interfacce API oggetto di verifica;
- utilizzo prioritario degli **strumenti di analisi dinamica già disponibili presso l'Amministrazione**, ove presenti e idonei allo scopo;
- configurazione ed esecuzione di test dinamici di tipo **black-box** e, ove richiesto, **autenticati**, al fine di analizzare il comportamento dell'applicazione in condizioni operative reali;

- analisi comportamentale dell'applicazione rispetto alla gestione degli input, delle sessioni e delle comunicazioni;
- validazione manuale dei risultati per ridurre i falsi positivi;
- classificazione delle vulnerabilità secondo standard di settore condivisi;
- supporto tecnico alle attività di remediation e verifica dell'efficacia delle azioni correttive (follow-up e re-testing), ove richiesto.

L'eventuale utilizzo di **strumenti del Fornitore** è consentito **esclusivamente previo accordo con l'Amministrazione**, in assenza di strumenti equivalenti già disponibili e **senza oneri aggiuntivi** per l'Amministrazione.

Tipologie di controlli di sicurezza

L'attività di analisi dinamica è svolta secondo le best practice internazionali e comprende, almeno, i seguenti ambiti di controllo:

- **Configurazione applicativa:** identificazione delle directory, delle risorse e delle pagine web coinvolte nel workflow applicativo, nonché delle superfici di esposizione esterne;
- **Autenticazione:** verifica dei meccanismi di autenticazione per accertare:
 - o l'utilizzo di canali di comunicazione sicuri per il transito delle credenziali;
 - o la presenza di politiche di enforcement delle credenziali (es. password deboli);
 - o l'adozione di contromisure contro attacchi a dizionario e brute force e la loro robustezza;
- **Autorizzazione:** verifica della possibilità di accesso non autorizzato a funzionalità o risorse protette, inclusi tentativi di elevazione dei privilegi o bypass dei controlli di accesso;
- **Validazione dei dati:** analisi della gestione degli input degli utenti al fine di individuare carenze nei meccanismi di validazione che possano condurre a vulnerabilità sfruttabili;
- **Gestione delle sessioni:** verifica dei meccanismi di creazione, mantenimento e terminazione delle sessioni applicative e della loro robustezza;
- **Gestione degli errori e logging:** analisi delle modalità di gestione degli errori applicativi e dei meccanismi di logging, con riferimento alla sicurezza delle informazioni e alla capacità di rilevare eventi anomali;
- **Comunicazioni e crittografia:** verifica delle comunicazioni dell'applicazione con client, database, directory service (es. LDAP) e altri sistemi esterni, inclusi i meccanismi crittografici adottati, ove applicabili.

Vulnerabilità e rischi analizzati

I controlli effettuati consentono di individuare e mitigare i principali rischi applicativi, tra cui, a titolo esemplificativo e non esaustivo:

- Injection (SQL, XPath, XML, XQuery);
- Cross-Site Scripting (XSS);
- Broken Authentication e Broken Access Control;
- Security Misconfiguration;
- Insecure Session Management;
- Sensitive Data Exposure;
- Insecure Deserialization;
- Insufficient Logging e Monitoring;
- esposizione non controllata di API e web service.

Standard e riferimenti metodologici

Il servizio di DAST è svolto dal Fornitore in coerenza con:

- OWASP Top 10;
- tassonomie e classificazioni di settore (CVE, CVSS, CWE);
- metodologie di sicurezza applicativa riconosciute a livello internazionale;
- **Linee Guida AgID per lo sviluppo del software sicuro nella Pubblica Amministrazione**, incluse le indicazioni su testing di sicurezza e secure by design.

Integrazione nei processi dell'Amministrazione

Ove previsto dall'Amministrazione, il servizio può essere integrato nei **processi di sviluppo, test e rilascio del software già adottati dalla stessa**, inclusi contesti DevOps e CI/CD, al fine di rendere strutturali le verifiche di sicurezza dinamica e supportare il miglioramento continuo della postura di sicurezza applicativa.

Il servizio è erogato dal Fornitore mediante l'impiego di **risorse professionali con competenze specialistiche in sicurezza applicativa**, operanti secondo i processi e gli strumenti dell'Amministrazione e, in caso siano utilizzati strumenti propri, come prima indicato, **senza oneri aggiuntivi** per la stessa.

3. Mobile Application Security Testing (MAST)

Descrizione del servizio

Il servizio di **Mobile Application Security Testing (MAST)** è un **servizio professionale di sicurezza applicativa** finalizzato alla valutazione della sicurezza delle applicazioni mobile dell'Amministrazione, sviluppate per sistemi operativi **Android** e **iOS**, mediante l'utilizzo

integrato di tecniche di **analisi statica**, **analisi dinamica** e **test manuali mirati**, incluse le **API** e i **servizi di backend** a supporto delle applicazioni.

Il servizio è erogato da **personale specializzato del Fornitore**, che opera **sull'infrastruttura applicativa e sugli ambienti dell'Amministrazione**, nel rispetto delle **metodologie, dei processi di sviluppo e delle regole operative adottate dalla stessa**.

L'attività è orientata a individuare vulnerabilità che possano compromettere la **riservatezza, l'integrità e la disponibilità** dei dati e dei servizi, considerando non solo l'applicazione mobile in sé, ma anche tutte le **interfacce verso sistemi esterni, servizi di backend e risorse collegate** che contribuiscono alla sicurezza complessiva della soluzione.

Ambito di applicazione

Il perimetro del servizio comprende l'analisi di:

- applicazioni mobile native o ibride per sistemi **Android** e **iOS**;
- componenti applicativi mobile distribuiti in formato **APK** o **IPA**;
- servizi di backend, API REST/SOAP e web service utilizzati dall'applicazione;
- meccanismi di integrazione dell'applicazione con altri sistemi informativi dell'Amministrazione o di terze parti.

Ove l'Amministrazione sia dotata di **linee guida interne per lo sviluppo del codice**, il servizio può essere utilizzato anche a supporto della **verifica di conformità** a tali linee guida.

Modalità di esecuzione del servizio

Il servizio è svolto dal Fornitore **in coordinamento con le strutture tecniche dell'Amministrazione** e prevede, almeno, le seguenti attività:

- definizione congiunta del perimetro di analisi in termini di applicazioni, piattaforme, componenti mobile e API di backend;
- utilizzo prioritario degli **strumenti di test e analisi già disponibili presso l'Amministrazione**, ove presenti e idonei allo scopo;
- esecuzione di **analisi statica** del codice e dei pacchetti applicativi (incluso reverse engineering e decompilazione, ove applicabile);
- esecuzione di **analisi dinamica** dell'applicazione in esecuzione su emulatori o dispositivi reali;
- test di sicurezza sulle **API e sui servizi di backend** utilizzati dall'applicazione mobile;
- simulazione di attacchi mirati per verificare l'effettiva sfruttabilità delle vulnerabilità individuate;

- validazione dei risultati e riduzione dei falsi positivi;
- classificazione delle vulnerabilità secondo criteri condivisi e supporto alle attività di remediation;
- verifica dell'efficacia delle azioni correttive (follow-up e re-testing), ove richiesto.

L'eventuale utilizzo di **strumenti del Fornitore** è consentito **esclusivamente previo accordo con l'Amministrazione**, in assenza di strumenti equivalenti già disponibili e **senza oneri aggiuntivi** per l'Amministrazione.

Tipologie di controlli di sicurezza

Le attività di MAST sono svolte secondo le best practice internazionali e comprendono, almeno, i seguenti ambiti di controllo:

- **Gestione dei dati sul dispositivo**: verifica delle modalità di memorizzazione dei dati sensibili (es. dati utente, credenziali, token) e delle protezioni adottate;
- **Comunicazioni**: analisi della sicurezza delle comunicazioni tra applicazione mobile e servizi di backend, inclusi protocolli e meccanismi di cifratura;
- **Autenticazione e autorizzazione**: verifica dei meccanismi di autenticazione, gestione delle sessioni e controllo degli accessi alle funzionalità dell'applicazione;
- **Policy di accesso a dati e funzionalità del dispositivo**: analisi delle autorizzazioni richieste e del loro utilizzo effettivo da parte dell'applicazione;
- **Protezione del codice e dell'applicazione**: verifica della resistenza a tecniche di reverse engineering, manomissione del codice e attacchi di privilege escalation;
- **Sicurezza delle API di backend**: analisi delle interfacce applicative esposte e della loro protezione rispetto ad accessi non autorizzati o utilizzi impropri.

Vulnerabilità e rischi analizzati

I controlli effettuati consentono di individuare vulnerabilità e rischi applicativi, tra cui, a titolo esemplificativo e non esaustivo:

- Insecure Data Storage;
- Insecure Communication;
- Insecure Authentication e Authorization;
- esposizione non controllata delle API;
- privilege escalation;
- utilizzo non sicuro di componenti o librerie di terze parti.

Alle vulnerabilità individuate è associato un **livello di severità**, anche mediante l'assegnazione di un punteggio numerico secondo lo standard **CVSS**, sulla base delle policy concordate con l'Amministrazione.

Standard e riferimenti metodologici

Il servizio di MAST deve essere svolto dal Fornitore in coerenza:

- con gli standard più comuni, quali:
 - o **OWASP Mobile Top 10**;
 - o **OWASP MASTG (Mobile Application Security Testing Guide)** e **OWASP MASVS**;
 - o tassonomie e classificazioni di settore (CVE, CVSS, CWE);
 - o normative e standard applicabili (inclusi GDPR e requisiti di sicurezza delle informazioni);

Integrazione nei processi dell'Amministrazione

Ove previsto dall'Amministrazione, il servizio può essere integrato nei **processi di sviluppo, test e rilascio delle applicazioni mobile**, inclusi contesti DevSecOps, al fine di:

- rendere strutturali le verifiche di sicurezza delle applicazioni mobile;
- fornire feedback tempestivi ai team di sviluppo;
- supportare il miglioramento continuo della sicurezza delle applicazioni pubblicate.

Il servizio è erogato dal Fornitore mediante l'impiego di **risorse professionali con competenze specialistiche in sicurezza applicativa**, operanti secondo i processi e gli strumenti dell'Amministrazione e, in caso siano utilizzati strumenti propri, come prima indicato, **senza oneri aggiuntivi** per la stessa.

4. Hardening

Descrizione del servizio

Il servizio di **Gestione Hardening** è un **servizio professionale di sicurezza dei sistemi e delle applicazioni**, finalizzato alla **riduzione strutturale della superficie di attacco** e alla mitigazione delle vulnerabilità attraverso l'applicazione, il mantenimento e il controllo di **configurazioni di sicurezza standardizzate**.

Il servizio è erogato da **personale specializzato del Fornitore**, che opera **sull'infrastruttura tecnologica dell'Amministrazione** e secondo le **metodologie, i processi operativi e le regole di governo della sicurezza adottate dalla stessa**, inclusi i processi di change e configuration management.

Le attività sono svolte utilizzando **prioritariamente gli strumenti, le piattaforme e le soluzioni già in uso presso l'Amministrazione**. L'eventuale utilizzo di **strumenti del Fornitore** è ammesso **esclusivamente ove necessario, previo accordo e autorizzazione dell'Amministrazione** e senza oneri aggiuntivi per la stessa.

Il servizio è progettato per garantire la conformità a **baseline di sicurezza riconosciute a livello internazionale**, quali, a titolo esemplificativo, **CIS Benchmarks, DISA STIGs** e i controlli di **Configuration Management** previsti dallo standard **NIST SP 800-53 Rev. 5 e aggiornamenti**, nonché per supportare i requisiti di sicurezza delle informazioni definiti dallo standard **ISO/IEC 27001:2022**.

Ambito di applicazione

Ai fini del presente Capitolato, le attività di **hardening** si applicano **esclusivamente ai sistemi, alle piattaforme e alle componenti tecnologiche che costituiscono o supportano soluzioni di sicurezza adottate dall'Amministrazione**, oggetto del presente servizio.

Restano escluse le attività di hardening riferite a sistemi informativi o applicativi dell'Amministrazione non riconducibili a soluzioni di sicurezza.

Il servizio di Gestione Hardening si applica, in funzione del contesto dell'Amministrazione, alle seguenti categorie di asset:

- sistemi operativi server e client (Windows, Linux/Unix, macOS);
- applicazioni, piattaforme middleware e database;
- dispositivi di rete e di sicurezza (es. firewall, proxy, IDS/IPS, WAF);
- ambienti virtualizzati, cloud e infrastrutture ibride;
- componenti e ambienti OT/IoT, ove presenti.

Si precisa che:

- **per sistemi operativi server** si intendono i sistemi utilizzati per l'erogazione di **servizi infrastrutturali, applicativi o di sicurezza**, tipicamente caratterizzati da elevati requisiti di **disponibilità, affidabilità e continuità operativa**.

Rientrano in tale ambito, a titolo esemplificativo e non esaustivo:

- o sistemi **Windows Server** e **Linux/Unix server** utilizzati per:
 - servizi di autenticazione e directory (es. domain controller);
 - application server e web server;
 - servizi API e middleware;
 - database e sistemi di integrazione applicativa;

- o server fisici o virtuali, inclusi ambienti **cloud o ibridi**, che supportano applicazioni e servizi istituzionali;
- o sistemi a supporto di funzioni di **sicurezza**, quali logging centralizzato, monitoraggio, backup e sistemi di controllo degli accessi.

Le attività di **hardening** sui sistemi server sono svolte con particolare attenzione agli **impatti sui servizi core**, prevedendo:

- o analisi preventiva delle configurazioni esistenti;
 - o applicazione controllata delle baseline di sicurezza;
 - o pianificazione delle attività in **finestre temporali adeguate**;
 - o verifiche post-intervento e, ove necessario, **procedure di ripristino (rollback)** delle configurazioni.
- **per sistemi operativi client** si intendono i sistemi installati sulle **postazioni di lavoro degli utenti dell'Amministrazione**, utilizzati per lo svolgimento delle attività operative e amministrative quotidiane.

Rientrano in tale ambito, a titolo esemplificativo e non esaustivo:

- o sistemi **Windows client** (es. Windows 10, Windows 11);
- o sistemi **macOS**;
- o eventuali sistemi **Linux desktop** adottati dall'Amministrazione;
- o postazioni di lavoro fisse o portatili gestite centralmente.

Le attività di **hardening** sui sistemi client sono normalmente caratterizzate da:

- o applicazione di configurazioni di sicurezza **standardizzate e centralizzate**;
- o definizione di criteri coerenti con i **ruoli degli utenti**;
- o maggiore grado di **automazione**;
- o impatto limitato sull'operatività dei singoli utenti.

Differenziazione delle modalità operative: pur rientrando nel medesimo servizio di **Gestione Hardening**, i sistemi operativi server e client sono oggetto di **modalità operative differenziate**, definite in funzione del ruolo dei sistemi, della criticità dei servizi supportati e delle esigenze di continuità operativa dell'Amministrazione. Tale distinzione consente di applicare le **configurazioni di sicurezza e le baseline di hardening** in modo **proporzionato e coerente** con il contesto operativo, nel rispetto dei processi di **change management** e delle **policy di sicurezza** adottate dall'Amministrazione.

Le attività tengono conto delle **Linee Guida AgID per lo sviluppo del software sicuro nella Pubblica Amministrazione**, con particolare riferimento alle **Linee Guida per la configurazione per adeguare la sicurezza del software di base (Allegato 3)**.

Modalità di esecuzione del servizio

Il servizio è svolto dal Fornitore **in coordinamento con le strutture tecniche dell'Amministrazione** e prevede, almeno, le seguenti attività:

- analisi dello stato attuale delle configurazioni dei sistemi e delle applicazioni (assessment iniziale);
- definizione e personalizzazione delle baseline di sicurezza, derivate, a titolo esemplificativo, da CIS Benchmarks, DISA STIGs e dai controlli di configurazione dello standard NIST SP 800-53;
- applicazione controllata delle configurazioni di hardening su sistemi, applicazioni e dispositivi, con attenzione alla continuità operativa dell'Amministrazione, anche mediante la pianificazione delle attività in finestre temporali adeguate e la predisposizione di procedure di verifica e di ripristino delle configurazioni, ove necessario;
- utilizzo, ove appropriato, di meccanismi di automazione per l'applicazione e la verifica delle configurazioni;
- monitoraggio delle configurazioni per l'individuazione di eventuali deviazioni rispetto alle baseline definite;
- aggiornamento periodico delle baseline e delle policy di sicurezza in funzione dell'evoluzione tecnologica e del contesto delle minacce;
- supporto alle attività di remediation e verifica dell'efficacia delle azioni correttive;
- produzione della documentazione tecnica e della reportistica a supporto delle attività svolte.

Tipologie di controlli di sicurezza

Le attività di hardening comprendono, a titolo esemplificativo e non esaustivo:

- disabilitazione di servizi, funzionalità e componenti non necessari;
- configurazione sicura di utenti, ruoli, privilegi e gruppi di accesso;
- rafforzamento dei meccanismi di autenticazione e gestione delle credenziali;
- configurazione sicura delle comunicazioni di rete e dei protocolli;
- impostazione dei parametri di logging e auditing a supporto delle attività di controllo e verifica;
- protezione delle configurazioni applicative e dei componenti critici.

Standard e riferimenti metodologici

Il servizio di Gestione Hardening è svolto in coerenza con standard quali:

- **CIS Benchmarks**, quali baseline di configurazione sicura;
- **DISA STIGs (Security Technical Implementation Guides)**;
- **NIST SP 800-53 Rev. 5 e successive patch**, in particolare i controlli di Configuration Management;
- **ISO/IEC 27001:2022**;
- **Linee Guida AgID per lo sviluppo del software sicuro nella Pubblica Amministrazione**, incluse le Linee Guida per la configurazione del software di base.

Integrazione nei processi dell'Amministrazione

Ove previsto dall'Amministrazione, il servizio può essere integrato nei **processi DevSecOps, di gestione della configurazione e di controllo continuo** già adottati dall'Amministrazione, al fine di garantire il mantenimento nel tempo delle configurazioni di sicurezza definite.

Il servizio è erogato dal Fornitore mediante l'impiego di **risorse professionali con competenze specialistiche in sicurezza applicativa**, operanti secondo i processi e gli strumenti dell'Amministrazione e, in caso siano utilizzati strumenti propri, come prima indicato, **senza oneri aggiuntivi** per la stessa.

5. Patching

Descrizione del servizio

Il servizio di **Gestione Patching** è un **servizio professionale di sicurezza dei sistemi e delle applicazioni** finalizzato alla **correzione tempestiva delle vulnerabilità** e al mantenimento di un adeguato livello di sicurezza dei sistemi informativi dell'Amministrazione, garantendo al contempo la **continuità operativa** dei servizi istituzionali.

Il servizio è erogato da **personale specializzato del Fornitore**, che opera **sull'infrastruttura tecnologica dell'Amministrazione** e nel rispetto delle **metodologie, dei processi organizzativi e delle regole operative adottate dalla stessa**, inclusi i processi di **change management e configuration management**.

L'approccio adottato è coerente con quanto definito da standard quali **NIST SP 800-40 Rev. 4 – Guide to Enterprise Patch Management Planning**, che qualifica il patching come attività di **manutenzione preventiva essenziale** per la riduzione del rischio e la protezione della missione dell'organizzazione.

Ambito di applicazione

Ai fini del presente Capitolato, le attività di **patching di sicurezza** sono riferite **esclusivamente alle soluzioni, ai sistemi e alle componenti tecnologiche di sicurezza adottate dall'Amministrazione**, incluse le piattaforme e i sistemi a supporto delle funzioni di protezione, monitoraggio, controllo degli accessi e gestione degli eventi di sicurezza.

Non rientrano nel perimetro del servizio le attività di patching riferite a sistemi informativi o applicativi generici dell'Amministrazione non riconducibili a soluzioni di sicurezza.

Il servizio di Gestione Patching si applica, in funzione del contesto dell'Amministrazione, a:

- sistemi operativi server e client;
- applicazioni e software di base;
- componenti middleware e database;
- dispositivi e infrastrutture IT, inclusi ambienti virtualizzati e cloud.

Si precisa che:

- per **sistemi operativi server** si intendono i sistemi utilizzati per l'erogazione di **servizi infrastrutturali, applicativi o di sicurezza**, tipicamente caratterizzati da elevati requisiti di **disponibilità, affidabilità e continuità operativa**.

Rientrano in tale ambito, a titolo esemplificativo e non esaustivo:

- o sistemi **Windows Server** e **Linux/Unix server** utilizzati per:
 - servizi di autenticazione e directory (es. domain controller);
 - application server e web server;
 - servizi API e middleware;
 - database e sistemi di integrazione applicativa;
- o server fisici o virtuali, inclusi ambienti cloud o ibridi, che supportano applicazioni e servizi istituzionali;
- o sistemi a supporto di funzioni di sicurezza (logging centralizzato, monitoraggio, backup, sistemi di controllo degli accessi).

Le attività di patching sui sistemi server sono svolte con particolare attenzione agli **impatti sui servizi core**, prevedendo test preventivi, pianificazione delle attività in finestre temporali adeguate, verifica post-installazione e, ove necessario, procedure di **ripristino (rollback)**.

- per **sistemi operativi client** si intendono i sistemi installati sulle **postazioni di lavoro degli utenti** dell'Amministrazione, utilizzati per lo svolgimento delle attività operative e amministrative quotidiane.
 - o Rientrano in tale ambito, a titolo esemplificativo e non esaustivo:
 - o sistemi **Windows client** (es. Windows 10, Windows 11);
 - o sistemi **macOS**;
 - o eventuali sistemi **Linux desktop** adottati dall'Amministrazione;
 - o postazioni di lavoro fisse o portatili gestite centralmente.

Le attività di patching sui sistemi client sono normalmente caratterizzate da un **elevato livello di automazione** e da una distribuzione su larga scala, mediante strumenti centralizzati, con l'obiettivo di garantire un'ampia copertura degli endpoint e ridurre il rischio derivante da vulnerabilità note, limitando l'impatto sull'operatività dei singoli utenti.

Differenziazione delle modalità operative: pur rientrando nel medesimo servizio di Gestione Patching, i sistemi operativi server e client sono oggetto di **modalità operative differenziate**, definite in funzione del ruolo dei sistemi, della criticità dei servizi supportati e delle esigenze di continuità operativa dell'Amministrazione. Tale distinzione consente di applicare il processo di patching in modo **proporzionato e coerente** con il contesto operativo, nel rispetto dei processi di change management e delle policy di sicurezza adottate dall'Amministrazione.

Le attività di patch management sono svolte utilizzando **prioritariamente gli strumenti di patch management già in uso presso l'Amministrazione**.

L'eventuale utilizzo di **strumenti del Fornitore** è ammesso **solo ove necessario, previa autorizzazione dell'Amministrazione e senza oneri aggiuntivi**.

Modalità di esecuzione del servizio

Il servizio è svolto dal Fornitore **in coordinamento con le strutture tecniche dell'Amministrazione** e comprende, almeno, le seguenti attività:

- **identificazione e analisi delle patch di sicurezza**, sulla base delle informazioni fornite dai vendor e delle basi dati sulle vulnerabilità;
- **classificazione e prioritizzazione delle patch** in funzione della criticità, dell'esposizione al rischio e dell'impatto sui servizi, in linea con i principi di gestione del rischio definiti dall'Amministrazione;
- **test preliminari** delle patch in ambienti di prova o di laboratorio, ove disponibili;

- **pianificazione dell'applicazione delle patch** in finestre temporali compatibili con le attività istituzionali core, nel rispetto delle esigenze di continuità operativa;
- **definizione e documentazione delle procedure di rollback**, da attivare in caso di impatti non previsti;
- **distribuzione automatizzata o controllata delle patch** mediante gli strumenti in uso presso l'Amministrazione;
- **monitoraggio dell'esito delle attività di patching** e gestione delle eventuali eccezioni;
- **reporting periodico** sullo stato di aggiornamento e di conformità dei sistemi.

Continuità operativa e gestione delle eccezioni

L'applicazione delle patch è effettuata in modo **controllato e graduale**, tenendo conto delle esigenze di continuità operativa dell'Amministrazione.

Ove necessario, sono previste:

- finestre temporali dedicate per l'esecuzione delle attività;
- procedure di verifica post-installazione;
- meccanismi di ripristino delle configurazioni precedenti (rollback).

Le eventuali eccezioni alla distribuzione delle patch sono **formalmente tracciate e motivate**, in conformità alle best practice di settore ed alle procedure dell'Amministrazione.

Standard e riferimenti metodologici

Il servizio di Gestione Patching è svolto in coerenza con le best practice di settore, quali a titolo esemplificativo:

- **NIST SP 800-40 Rev. 4 – Guide to Enterprise Patch Management Planning**
- **CIS Critical Security Controls**, in particolare i controlli relativi al patch management automatizzato dei sistemi operativi e delle applicazioni
- **ISO/IEC 27001:2022**, in relazione alla gestione delle vulnerabilità tecniche

Integrazione nei processi dell'Amministrazione

Ove previsto dall'Amministrazione, il servizio può essere integrato nei **processi DevSecOps e nelle pipeline CI/CD** adottate dall'Amministrazione, al fine di rendere strutturale e ripetibile la gestione degli aggiornamenti di sicurezza e di supportare il miglioramento continuo della postura di sicurezza.

Il servizio è erogato dal Fornitore mediante l'impiego di **risorse professionali con competenze specialistiche in sicurezza applicativa**, operanti secondo i processi e gli strumenti

dell'Amministrazione e, in caso siano utilizzati strumenti propri, come prima indicato, **senza oneri aggiuntivi** per la stessa.

6. Definizione di processi e procedure per la verifica dell'integrità dei sistemi

Descrizione del servizio

Il servizio di **Definizione di processi e procedure per la verifica dell'integrità dei sistemi** è un **servizio professionale di sicurezza dei sistemi e delle applicazioni** finalizzato alla **progettazione, formalizzazione e mantenimento** di processi e procedure operative per il **monitoraggio e la verifica dell'integrità** dei sistemi informativi dell'Amministrazione.

L'obiettivo del servizio è consentire all'Amministrazione di **rilevare tempestivamente modifiche non autorizzate**, manomissioni, alterazioni delle configurazioni o violazioni dell'integrità di **software, firmware, configurazioni e informazioni**, in coerenza con le principali best practice di settore quali il controllo **SI-7 – Software, Firmware and Information Integrity** dello standard **NIST SP 800-53 Rev. 5**.

Il servizio è erogato da **personale specializzato del Fornitore**, che opera **sull'infrastruttura e secondo i processi dell'Amministrazione**, nel rispetto delle **policy di sicurezza, dei processi di change management e incident management** adottati dalla stessa.

Ambito di applicazione

Il servizio si applica ai **sistemi IT dell'Amministrazione**, inclusi, a titolo esemplificativo e non esaustivo:

- sistemi operativi server e client;
- dispositivi di rete e di sicurezza;
- applicazioni e servizi applicativi;
- database e archivi informativi;
- configurazioni di sistema e di sicurezza.

L'ambito è definito in funzione degli **asset critici** individuati dall'Amministrazione, in coerenza con le raccomandazioni delle best practice internazionali quali **CIS Critical Security Controls** in materia di inventario degli asset, configurazioni sicure e monitoraggio continuo.

Modalità di esecuzione del servizio

Il servizio è svolto dal Fornitore **in coordinamento con le strutture tecniche dell'Amministrazione** e comprende, almeno, le seguenti attività:

- analisi dello **stato attuale** delle misure di verifica dell'integrità e dei controlli già in essere;
- identificazione degli **asset critici** da sottoporre a verifica di integrità;
- definizione degli **obiettivi di controllo**, quali:
 - o rilevamento di modifiche non autorizzate;
 - o protezione delle configurazioni di sicurezza;
 - o individuazione di manomissioni o compromissioni;
- progettazione e formalizzazione di **policy e procedure** per:
 - o monitoraggio delle modifiche;
 - o validazione delle configurazioni;
 - o gestione degli eventi e degli incidenti di integrità;
- definizione di **ruoli e responsabilità** per il monitoraggio, l'analisi e la risposta agli eventi;
- supporto all'implementazione di **strumenti di verifica dell'integrità**, utilizzando prioritariamente quelli già in uso presso l'Amministrazione;
- test e validazione delle procedure mediante **simulazione di scenari di modifica o manomissione**;
- formazione del personale IT dell'Amministrazione;
- revisione periodica delle procedure in funzione dell'evoluzione del contesto tecnologico e delle minacce.

Integrazione con i processi di sicurezza

Le procedure di verifica dell'integrità sono progettate per essere **integrate nei processi di sicurezza dell'Amministrazione**, inclusi:

- change management e configuration management;
- incident response e gestione degli eventi di sicurezza;
- monitoraggio centralizzato e correlazione degli eventi.

Ove previsto, il servizio può essere integrato con piattaforme di monitoraggio e risposta agli incidenti, quali SIEM e SOAR, al fine di automatizzare la generazione degli alert e supportare una risposta tempestiva agli incidenti di integrità, in coerenza con le best practice e i controlli previsti dagli standard NIST e CIS.

Continuità operativa e miglioramento continuo

Il servizio supporta l'Amministrazione nel mantenimento nel tempo di un adeguato livello di **integrità dei sistemi**, attraverso:

- monitoraggio continuo delle modifiche;
- revisione periodica delle baseline di riferimento;
- aggiornamento delle procedure in caso di nuove minacce o variazioni normative;
- supporto agli audit e alle attività di verifica di conformità.

Il Fornitore deve definire e documentare i processi e le procedure per la verifica dell'integrità dei dati e dei sistemi informativi, assicurandone la coerenza con i requisiti di sicurezza, disponibilità e affidabilità previsti da standard quali ISO/IEC 27001 e dalla normativa applicabile ai dati e ai servizi delle amministrazioni.

Standard e riferimenti metodologici

Il servizio è svolto in coerenza con i principali standard e framework, quali:

- **NIST SP 800-53 Rev. 5 – SI-7 Software, Firmware and Information Integrity;**
- **ISO/IEC 27001:2022**, con riferimento ai controlli per la protezione dell'integrità delle informazioni e al monitoraggio dell'efficacia dei controlli;
- **CIS Critical Security Controls**, in particolare i controlli relativi a configurazioni sicure, monitoraggio delle modifiche e gestione degli asset;
- **PCI DSS**, che prevede l'adozione di meccanismi di monitoraggio dell'integrità dei file e delle configurazioni critiche

Integrazione nei processi DevSecOps (opzionale)

Ove previsto dall'Amministrazione, alcune attività di verifica dell'integrità, limitatamente alla validazione delle configurazioni e degli artefatti in fase di rilascio, possono essere integrate nei processi DevSecOps e nelle pipeline CI/CD.

Resta inteso che le attività di monitoraggio continuo dell'integrità dei sistemi in esercizio costituiscono controlli di sicurezza operativa e sono gestite al di fuori delle pipeline di sviluppo.

Per tutte le attività gestite dal Fornitore nell'ambito del presente paragrafo, lo stesso dovrà condurre **SAL periodici settimanali** (o con diversa periodicità concordata con l'Amministrazione), e produrre la relativa documentazione in formato:

- **dettagliato** per le strutture operative;
- **executive** per le strutture direttive.

Inoltre, in caso di richieste di chiarimenti sull'operato da parte dell'Amministrazione, formalizzate attraverso i canali di comunicazione previsti o concordati nell'ambito del Contratto Esecutivo, il Fornitore dovrà fornire riscontro entro 2 giorni lavorativi.

2.4.2 Deliverable

Il presente paragrafo descrive i **deliverable minimi** che il Fornitore dovrà produrre nell'ambito del servizio di *Sicurezza dei sistemi e delle applicazioni*, in coerenza con le attività descritte nel presente capitolo e con quanto definito nel Piano di Lavoro Generale e nei singoli Contratti Esecutivi.

I deliverable sono finalizzati a supportare l'Amministrazione nelle attività di governance, valutazione del rischio, prioritizzazione degli interventi e miglioramento continuo della postura di sicurezza.

ID	SERVIZIO DI RIFERIMENTO	TITOLO	DESCRIZIONE	SLA
SA_1	SAST	Report tecnico SAST	Report delle vulnerabilità rilevate tramite analisi statica del codice, con classificazione del rischio e raccomandazioni di remediation	Entro 5 giorni lavorativi dalla conclusione delle attività
SA_2	SAST	Executive summary SAST	Sintesi dei risultati SAST per strutture direzionali	Contestuale al report tecnico
SA_3	SAST	Evidenze e checklist di remediation	Evidenze tecniche e checklist a supporto delle attività correttive	Contestuale al report tecnico
SA_4	DAST	Report tecnico DAST	Report delle vulnerabilità rilevate tramite analisi dinamica, incluse prove di concetto ove applicabili	Entro 3-10 giorni lavorativi dalla conclusione delle attività
SA_5	DAST	Executive summary DAST	Sintesi dei risultati DAST per strutture direzionali	Contestuale al report tecnico
SA_6	DAST	Documento di supporto alla remediation	Documento tecnico a supporto delle attività di correzione	Entro 5 giorni lavorativi dalla consegna del report
SA_7	MAST	Mobile Security Report	Report di sicurezza delle applicazioni mobile (Android/iOS), incluse API di backend	Entro 10 giorni lavorativi dalla conclusione delle attività

ID	SERVIZIO DI RIFERIMENTO	TITOLO	DESCRIZIONE	SLA
SA_8	MAST	Executive summary MAST	Sintesi dei risultati MAST per strutture direzionali	Contestuale al report tecnico
SA_9	MAST	Evidenze e checklist di remediation	Evidenze tecniche e checklist a supporto delle attività correttive	Contestuale al report tecnico
SA_10	Hardening	Report di assessment iniziale	Documento di analisi dello stato configurativo dei sistemi oggetto di hardening	Entro 10 giorni lavorativi dall'avvio delle attività
SA_11	Hardening	Baseline di sicurezza	Baseline di configurazione sicura personalizzate per il contesto della PA	Entro 5 giorni lavorativi dalla conclusione dell'assessment o diversa tempistica concordata con l'Amministrazione
SA_12	Hardening	Report di conformità	Report di verifica della conformità dei sistemi alle baseline applicabili	Entro 3 giorni lavorativi dalla conclusione delle attività
SA_13	Patching	Piano di aggiornamento software	Piano delle attività di patching concordate	Entro 5 giorni lavorativi dalla pianificazione
SA_14	Patching	Report di distribuzione patch	Report delle patch applicate e delle eccezioni gestite	Secondo periodicità concordata (mensile o ad evento)
SA_15	Patching	Registro delle eccezioni	Registro delle eccezioni al piano di patching approvate dall'Amministrazione	Aggiornamento continuativo
SA_16	Integrità sistemi	Policy e procedure di verifica	Policy e procedure formalizzate per la verifica dell'integrità dei sistemi	Entro 20 giorni lavorativi dall'avvio delle attività

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

ID	SERVIZIO DI RIFERIMENTO	TITOLO	DESCRIZIONE	SLA
SA_17	Integrità sistemi	Report di verifica periodica	Report delle verifiche di integrità effettuate	Secondo periodicità concordata con l'Amministrazione
SA_18	Tutti i servizi	SAL periodico	Stato Avanzamento Lavori in formato operativo ed executive	Settimanale o mensile , secondo Piano di Lavoro
SA_19	Tutti i servizi	Risposte a richieste di chiarimento	Riscontro a richieste di chiarimento dell'Amministrazione	Entro 48 ore lavorative

Ove richiesto dall'Amministrazione, i deliverable di cui al presente paragrafo possono essere rappresentati anche mediante viste riepilogative o cruscotti, realizzati utilizzando esclusivamente gli strumenti già in uso presso la stessa o in formato statico, senza introduzione di piattaforme dedicate o oneri aggiuntivi.

L'Amministrazione valuterà i deliverable entro **5 giorni lavorativi** dalla consegna. In caso di richieste di modifica, il Fornitore dovrà aggiornare/modificare i deliverable entro **5 giorni lavorativi** dalla comunicazione della PA, salvo diversa tempistica concordata.

Tutte le tempistiche dovranno essere indicate nel Piano di Lavoro Generale.

Gli adempimenti indicati nel presente paragrafo e ad esso collegati sono valutati ai fini di rilievi/penali in:

- 4.1 IQ01 – *Rispetto di una scadenza contrattuale;*
- 4.2 IQ02 – *Adeguatezza delle figure professionali proposte per la erogazione dei servizi;*
- 4.5 IQ05 - *Turnover del personale impiegato nella fornitura;*
- 4.6 IQ06 – *Impegni assunti in offerta tecnica;*
- 4.14 IQ14 – *Copertura del perimetro assegnato;*
- 4.15 IQ15 – *Completezza delle attività di sicurezza applicativa e infrastrutturale;*
- 4.22 IQ22 – *Rilievi su obbligazioni contrattuali non presidiate.*

2.4.3 Figure professionali coinvolte

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 al capitolo 3 *Risorse da impiegare nell'esecuzione dei servizi*):

- Security Principal;
- Cloud Security Expert;
- OT/IoT Security Expert;
- Senior Security Consultant;
- Security Analyst;
- Security Specialist;
- Information Security Manager;
- Senior Penetration Tester;
- Junior Penetration Tester;
- Security Engineer;
- Network Security Engineer.

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

2.4.4 Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento di tutti i servizi è: **Giorno/Persona**.

La modalità di remunerazione di tutti i servizi è: **a tempo/spesa oppure a corpo**.

In fase di offerta è richiesto al Concorrente di esprimere un prezzo per giorno/persona per ogni figura professionale prevista. I prezzi espressi saranno riferiti rispettivamente a:

- 8 ore lavorative complessive nella fascia oraria feriale Lun-Sab 8.00-20.00 (fascia standard);
- 8 ore lavorative complessive nella fascia oraria Lun-Sab 20.00-7.00 o la domenica o nei giorni festivi (fascia straordinaria).

In sede di Piano dei fabbisogni, l'Amministrazione definirà i deliverables richiesti e le risorse necessarie, indicando quindi il mix necessario per le attività richieste, in un'ottica di coerenza e proporzionalità.

2.5 Conduzione operativa dei sistemi di sicurezza

La **Conduzione operativa dei sistemi di sicurezza** è un **ambito funzionale** finalizzato a supportare la **gestione operativa, sistemistica e applicativa**, dei sistemi e delle piattaforme di sicurezza in uso presso l'Amministrazione, assicurandone il corretto funzionamento tecnico, l'aggiornamento, la coerenza configurativa e l'integrazione con il contesto infrastrutturale e applicativo esistente.

Il servizio è rivolto alla **conduzione operativa dei sistemi di sicurezza**, intesi come componenti del sistema informativo dell'Amministrazione, ed è svolto da **figure professionali specialistiche** che operano **sugli strumenti di sicurezza della PA**, in affiancamento alle strutture interne competenti.

Il servizio **non si configura come servizio di sicurezza gestita né come SOC**, e non comporta l'assunzione di responsabilità in merito al livello di sicurezza complessivo del sistema informativo, che resta in capo all'Amministrazione.

Il servizio si applica ai sistemi e alle piattaforme di sicurezza adottati dall'Amministrazione, quali, a titolo esemplificativo e non esaustivo:

- firewall e sistemi di sicurezza perimetrale;
- piattaforme di gestione degli accessi e delle identità;
- sistemi di protezione degli endpoint e dei server;
- piattaforme di raccolta, correlazione e gestione dei log di sicurezza (es. SIEM);
- soluzioni di orchestrazione e automazione a supporto dei sistemi di sicurezza;
- altri apparati e applicazioni di sicurezza in uso presso l'Amministrazione.

2.5.1 Attività previste

Il servizio comprende attività di **conduzione operativa, sistemistica e applicativa**, dei sistemi di sicurezza dell'Amministrazione, che possono includere:

- **monitoraggio tecnico e applicativo** dello stato dei sistemi di sicurezza, limitatamente agli aspetti di **funzionamento, disponibilità e corretta configurazione**;
- **installazione, configurazione iniziale e presa in carico operativa** dei sistemi di sicurezza;
- **aggiornamento e gestione delle versioni software** e delle **configurazioni applicative** dei sistemi di sicurezza;
- **gestione operativa delle policy e delle configurazioni** sui sistemi di sicurezza, **su indicazione e previa autorizzazione dell'Amministrazione**;
- **implementazione di modifiche configurative** richieste dall'Amministrazione (ad esempio: inserimento o modifica di **regole firewall**, aggiornamento di **policy**, configurazione dei **meccanismi di logging**);
- **gestione delle utenze e dei profili di accesso amministrativi** ai sistemi di sicurezza;
- **supporto alla corretta integrazione** dei sistemi di sicurezza con gli altri sistemi ICT dell'Amministrazione;
- **conduzione operativa ordinaria** dei sistemi di sicurezza, inclusa la **verifica del corretto funzionamento** e della **coerenza delle configurazioni applicative**;
- **supporto alla produzione e all'aggiornamento della documentazione tecnica e operativa** relativa ai sistemi di sicurezza;

- **supporto tecnico** alle strutture dell'Amministrazione in occasione di **verifiche, audit o attività di compliance tecnica**.

Le attività comprendono sia attività di **conduzione operativa**, intese come **mantenimento in esercizio e gestione ordinaria** dei sistemi di sicurezza, sia attività di **gestione operativa su richiesta dell'Amministrazione**, finalizzate all'implementazione di **modifiche, configurazioni o interventi puntuali** sui sistemi stessi.

In ogni caso, tali attività **non includono l'assunzione di decisioni in materia di sicurezza**, che restano **in capo all'Amministrazione**.

Nell'ambito del servizio:

- l'Amministrazione mantiene il **governo delle decisioni in materia di sicurezza**, incluse l'**analisi degli eventi**, la **valutazione del rischio** e la **gestione degli incidenti di sicurezza**;
- il Fornitore opera sui sistemi di sicurezza **in qualità di gestore sistemistico e applicativo**, eseguendo **esclusivamente le attività richieste e autorizzate** dall'Amministrazione;
- le attività di **analisi degli eventi di sicurezza, incident management, threat intelligence, investigazione e risposta agli incidenti** non rientrano nel perimetro del servizio.

Il servizio è erogato:

- utilizzando i **processi, gli strumenti e le piattaforme messi a disposizione dall'Amministrazione**;
- in modalità **continuativa o su richiesta**, secondo quanto definito nel **Piano dei fabbisogni** e nel **Piano di lavoro**;
- in **orario di servizio standard**, con eventuali estensioni in **fascia straordinaria**, ove richiesto dall'Amministrazione;
- in modalità **on-site e/o da remoto**, in funzione delle esigenze operative e organizzative.

Il servizio è strutturato per adattarsi alle diverse esigenze dell'Amministrazione.

Il Fornitore può avvalersi di **propri strumenti e soluzioni tecniche** a supporto dell'erogazione del servizio (ad esempio strumenti di accesso remoto, **console di amministrazione** o strumenti di supporto operativo), a condizione che:

- tali strumenti siano **preventivamente autorizzati dall'Amministrazione**;
- il loro utilizzo sia **conforme alle politiche di sicurezza e di accesso** dell'Amministrazione;
- non comportino **oneri aggiuntivi**, diretti o indiretti, per l'Amministrazione;
- non introducano **vincoli di lock-in tecnologico**;
- non comportino la **memorizzazione, elaborazione o trasmissione di dati dell'Amministrazione al di fuori degli ambiti autorizzati**;

- siano **pienamente dismettibili e sostituibili** su richiesta dell'Amministrazione.

L'Amministrazione si riserva in ogni momento la facoltà di richiedere la **dismissione o la sostituzione** degli strumenti utilizzati dal Fornitore.

Per tutte le attività gestite dal Fornitore nell'ambito del presente paragrafo, lo stesso dovrà condurre **SAL periodici settimanali** (o con diversa periodicità concordata con l'Amministrazione), e produrre la relativa documentazione in formato:

- **dettagliato** per le strutture operative;
- **executive** per le strutture direttive.

Inoltre, in caso di richieste di chiarimenti sull'operato da parte dell'Amministrazione, formalizzate attraverso i canali di comunicazione previsti o concordati nell'ambito del Contratto Esecutivo, il Fornitore dovrà fornire riscontro entro 2 giorni lavorativi.

2.5.2 Deliverable

Il presente paragrafo descrive i **deliverable minimi** che il Fornitore dovrà produrre nell'ambito del servizio di *Conduzione operativa dei sistemi di sicurezza*, in coerenza con le attività descritte nel presente capitolo e con quanto definito nel Piano di Lavoro Generale e nei singoli Contratti Esecutivi.

I deliverable sono finalizzati a supportare l'Amministrazione nelle attività di governance, valutazione del rischio, prioritizzazione degli interventi e miglioramento continuo della postura di sicurezza.

ID	TITOLO	DESCRIZIONE	SLA
SO_1	Registro delle attività di Conduzione operativa dei sistemi di sicurezza	Registro strutturato delle attività di conduzione e gestione operativa svolte sui sistemi di sicurezza dell'Amministrazione (configurazioni applicate, aggiornamenti effettuati, interventi operativi), mantenuto utilizzando gli strumenti dell'Amministrazione o formati concordati.	Aggiornamento continuativo con consolidamento mensile , secondo Piano di Lavoro Generale
SO_2	Documentazione di configurazione dei sistemi di sicurezza	Documentazione tecnica aggiornata relativa alle configurazioni operative dei sistemi di sicurezza (policy, regole, parametri applicativi), prodotta o aggiornata a seguito delle attività svolte.	Entro 5 giorni lavorativi dalla modifica o secondo secondo Piano di Lavoro Generale

ID	TITOLO	DESCRIZIONE	SLA
SO_3	Report tecnico di stato dei sistemi di sicurezza	Report tecnico sullo stato operativo dei sistemi di sicurezza, limitatamente agli aspetti di funzionamento e configurazione, senza analisi di eventi o valutazioni di rischio.	Mensile , salvo diversa indicazione nel secondo Piano di Lavoro Generale
SO_4	Evidenze delle attività svolte	Evidenze tecniche a supporto delle attività di Conduzione operativa dei sistemi di sicurezza (estratti configurativi, log di sistema, report di esecuzione), prodotte utilizzando gli strumenti dell'Amministrazione o modalità concordate.	Entro 5 giorni lavorativi dalla richiesta dell'Amministrazione
SO_5	Verballi di coordinamento tecnico	Verballi degli incontri di coordinamento tecnico-operativo con l'Amministrazione, finalizzati all'allineamento sulle attività svolte e pianificate.	Entro 3 giorni lavorativi dall'incontro
SO_6	Piano di Conduzione operativa dei sistemi di sicurezza	Documento di avvio che descrive perimetro dei sistemi di sicurezza presi in carico, modalità operative e interazioni con le strutture dell'Amministrazione.	Entro 10 giorni lavorativi dall'avvio del servizio o dalla presa in carico
SO_7	SAL periodico	Stato Avanzamento Lavori in formato operativo ed executive , comprensivo delle attività svolte nel periodo di riferimento.	Settimanale o mensile , secondo Piano di Lavoro
SO_8	Risposte a richieste di chiarimento	Riscontri tecnici a richieste di chiarimento dell'Amministrazione su attività o deliverable prodotti.	Entro 48 ore lavorative

L'Amministrazione valuterà i deliverable entro **5 giorni lavorativi** dalla consegna. In caso di richieste di modifica, il Fornitore dovrà aggiornare/modificare i deliverable entro **5 giorni lavorativi** dalla comunicazione della PA, salvo diversa tempistica concordata.

Tutte le tempistiche dovranno essere indicate nel Piano di Lavoro Generale.

Gli adempimenti indicati nel presente paragrafo e ad esso collegati sono valutati ai fini di rilievi/penali in:

- 4.1 IQ01 – *Rispetto di una scadenza contrattuale;*
- 4.2 IQ02 – *Adeguatezza delle figure professionali proposte per la erogazione dei servizi;*

- 4.5 IQ05 - Turnover del personale impiegato nella fornitura;
- 4.6 IQ06 – Impegni assunti in offerta tecnica;
- 4.18 IQ18 – Copertura del perimetro assegnato;
- 4.26 IQ26 – Rilievi su obbligazioni contrattuali non presidiate.

2.5.3 Figure professionali coinvolte

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 al capitolo 3 *Risorse da impiegare nell'esecuzione dei servizi*):

- Security Principal;
- Cloud Security Expert;
- OT/IoT Security Expert;
- Security Analyst;
- Security Specialist;
- Information Security Manager;
- Security Engineer;
- Network Security Engineer.

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

2.5.4 Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento di tutti i servizi è: **Giorno/Persona**.

La modalità di remunerazione di tutti i servizi è: **a tempo/spesa oppure a corpo**.

In fase di offerta è richiesto al Concorrente di esprimere un prezzo per giorno/persona per ogni figura professionale prevista. I prezzi espressi saranno riferiti rispettivamente a:

- 8 ore lavorative complessive nella fascia oraria feriale Lun-Sab 8.00-20.00 (fascia standard);
- 8 ore lavorative complessive nella fascia oraria Lun-Sab 20.00-7.00 o la domenica o nei giorni festivi (fascia straordinaria).

In sede di Piano dei fabbisogni, l'Amministrazione definirà i deliverables richiesti e le risorse necessarie, indicando quindi il mix necessario per le attività richieste, in un'ottica di coerenza e proporzionalità.

2.6 Supporto specialistico

Il presente paragrafo disciplina il servizio di Supporto specialistico, volto a mettere a disposizione dell'Amministrazione un insieme flessibile e modulare di competenze professionali ad elevata specializzazione, attivabili in funzione di specifiche esigenze tecniche, operative o evolutive che emergano nel corso dell'esecuzione dei Contratti Esecutivi.

Il servizio è concepito per integrare e completare il portafoglio dei servizi disciplinati nel presente Capitolato, consentendo all'Amministrazione di avvalersi, ove necessario, di supporto qualificato su ambiti non interamente riconducibili ai singoli servizi tipizzati, ovvero su iniziative caratterizzate da particolare complessità o specificità tecnica.

Il Supporto specialistico si configura come servizio trasversale e su richiesta, erogato in affiancamento alle strutture dell'Amministrazione, nel rispetto delle regole di governo, dei processi organizzativi e delle modalità operative dalla stessa adottate, senza sovrapporsi ai servizi specifici già previsti né configurarsi come servizio gestito o di natura continuativa autonoma.

2.6.1 Attività previste

Nell'ambito del servizio di Supporto specialistico, il Fornitore fornisce, su richiesta dell'Amministrazione, attività professionali ad elevato contenuto tecnico e specialistico, finalizzate a supportare iniziative complesse o specifiche che richiedano competenze avanzate in ambito di cybersecurity, architetture tecnologiche e trasformazione dei sistemi.

Le attività sono svolte esclusivamente su indicazione e previa autorizzazione dell'Amministrazione e si configurano come supporto tecnico-specialistico e affiancamento operativo alle strutture interne, senza assunzione di responsabilità decisionali, di governo dei processi o di gestione end-to-end dei servizi.

1. Supporto specialistico per la migrazione tecnologica

Il servizio può includere attività di supporto specialistico per la gestione di iniziative di migrazione tecnologica di sistemi, dati o ambienti applicativi, ivi incluse, a titolo esemplificativo e non esaustivo:

- analisi preliminare dei sistemi e delle soluzioni esistenti;
- supporto alla definizione dei requisiti funzionali e di sicurezza;
- supporto alla definizione della soluzione target e del piano di migrazione;
- affiancamento operativo alle attività di migrazione;
- supporto alla gestione dei rischi e al coordinamento delle attività di migrazione nel rispetto dei processi dell'Amministrazione;
- verifica tecnica e validazione delle configurazioni a valle della migrazione.

2. Supporto specialistico per l'integrazione tecnologica

Il servizio può includere attività di supporto specialistico per la progettazione e realizzazione di integrazioni tecnologiche tra sistemi, piattaforme o servizi, incluse:

- analisi dei requisiti di integrazione e dei sistemi coinvolti;
- supporto alla progettazione delle modalità di integrazione e delle architetture di collegamento;
- affiancamento operativo alle attività di implementazione tecnica;
- supporto alla centralizzazione, normalizzazione e correlazione delle informazioni di sicurezza;
- verifica del corretto funzionamento delle integrazioni e supporto alla risoluzione di eventuali criticità.

3. Supporto specialistico per la progettazione e realizzazione di architetture di cybersecurity e continuità operativa

Il servizio può includere attività di supporto specialistico per la progettazione, revisione o realizzazione di architetture di cybersecurity e di continuità operativa, quali:

- analisi delle architetture esistenti e dei requisiti di sicurezza e resilienza;
- supporto alla definizione di architetture di sicurezza multilivello;
- supporto alla progettazione di soluzioni di continuità operativa e disaster recovery;
- affiancamento operativo alle attività di implementazione delle soluzioni;
- supporto alla verifica tecnica, ai test di resilienza e alla validazione delle misure adottate.

4. Supporto specialistico per la sicurezza di soluzioni basate su tecnologie di intelligenza artificiale e machine learning

Il servizio di Supporto specialistico per la sicurezza di soluzioni basate su tecnologie di Intelligenza Artificiale e Machine Learning (AI/ML) è finalizzato a supportare l'Amministrazione nella valutazione, analisi e mitigazione dei rischi di sicurezza connessi all'impiego di motori, modelli, pipeline e servizi applicativi AI/ML già adottati o in corso di adozione.

Il servizio è orientato alla securizzazione tecnica delle componenti AI/ML e non comprende attività di progettazione funzionale, sviluppo, addestramento dei modelli, definizione delle strategie di adozione dell'AI o attività di governo e indirizzo strategico, che restano integralmente in capo all'Amministrazione.

Le attività sono erogate in modalità di supporto tecnico-specialistico e affiancamento operativo, nel rispetto dei processi, delle policy e delle architetture dell'Amministrazione, e sono coerenti con i requisiti normativi e regolatori applicabili sia nazionali che europei.

Nell'ambito del servizio, il Fornitore supporta l'Amministrazione nello svolgimento delle seguenti attività.

Analisi della superficie di esposizione e degli asset AI/ML

- Supporto alla mappatura delle componenti AI/ML in scope, considerando anche le relazioni di dipendenza e della supply chain delle stesse, quali, a titolo esemplificativo:
 - o modelli AI/ML;
 - o pipeline di training e inferenza;
 - o dataset utilizzati;
 - o servizi applicativi e API di accesso;
 - o integrazioni con sistemi esterni o di terze parti.
- Identificazione delle principali superfici di esposizione e dei punti di interazione con l'ecosistema applicativo e infrastrutturale dell'Amministrazione.

Valutazione dei rischi di sicurezza delle soluzioni AI/ML

- Supporto all'analisi dei rischi specifici di sicurezza delle soluzioni AI/ML, con particolare riferimento a:
 - o esposizione e protezione e tracciabilità delle basi dati e dei dataset di training, validazione, test e inferenza, nonché delle fonti di addestramento;
 - o sicurezza degli accessi e delle identità applicative;
 - o protezione delle API e dei servizi di interfaccia;
 - o integrità dei modelli e delle pipeline;
 - o potenziali vulnerabilità derivanti da configurazioni non sicure.
- Contestualizzazione dei rischi rispetto al contesto operativo dell'Amministrazione e agli impatti sulla sicurezza dei servizi.

Integrazione con le attività di Continuous Vulnerability Management

Le attività di supporto alla sicurezza delle soluzioni AI/ML si integrano con i processi di Continuous Vulnerability Management previsti nel presente Capitolato, senza duplicazione delle attività già disciplinate nei relativi paragrafi.

Il contributo del servizio AI/ML è finalizzato a supportare la contestualizzazione e l'interpretazione delle evidenze di rischio relative a componenti che impiegano tecnologie di Intelligenza Artificiale e Machine Learning.

Definizione di misure tecniche di mitigazione

- Supporto all'individuazione e alla definizione di misure tecniche e procedurali di mitigazione, coerenti con:
 - o le architetture e i controlli di sicurezza dell'Amministrazione;
 - o le best practice di sicurezza applicativa e infrastrutturale;
 - o i requisiti normativi e regolatori applicabili.

Le misure tecniche di mitigazione possono prevedere, ove già disponibili o adottati dall'Amministrazione, l'utilizzo di strumenti e soluzioni tecnologiche a supporto delle attività di sicurezza, quali strumenti di analisi, verifica, monitoraggio o controllo delle componenti AI/ML in scope.

Nell'ambito delle attività, il Fornitore può supportare l'Amministrazione nell'individuazione e nella valutazione di eventuali strumenti tecnologici utili a rafforzare le misure di sicurezza delle soluzioni AI/ML in scope, limitandosi alla definizione delle caratteristiche tecniche, dei requisiti di sicurezza e delle modalità di integrazione con il contesto applicativo e infrastrutturale dell'Amministrazione.

Nell'ambito delle misure tecniche di mitigazione, il Fornitore supporta l'Amministrazione nella verifica dell'auditabilità tecnica delle soluzioni AI/ML, inclusa la capacità di produrre evidenze e report di sicurezza in formati aperti, verificabili e privi di dipendenze da strumenti proprietari non documentati.

- Supporto alla verifica tecnica delle misure di mitigazione proposte, senza assunzione di responsabilità esecutiva.

5. Attività trasversali di supporto specialistico

Il servizio può altresì includere attività di supporto specialistico per:

- analisi tecniche e valutazioni di soluzioni;
- approfondimenti tematici su specifici ambiti di cybersecurity;
- affiancamento operativo a strutture interne su iniziative puntuali o caratterizzate da elevata complessità tecnica.

Tutte le attività di Supporto specialistico sono erogate nel rispetto dei processi, delle metodologie e degli strumenti adottati dall'Amministrazione e non comportano in alcun caso l'erogazione di servizi gestiti, l'assunzione di responsabilità end-to-end o lo svolgimento di funzioni di governance.

Il servizio di Supporto specialistico è erogato secondo un modello flessibile e modulare, attivabile su richiesta dell'Amministrazione in funzione di specifiche esigenze tecniche, operative o progettuali che richiedano competenze specialistiche non riconducibili ai singoli servizi tipizzati del Capitolato.

L'attivazione del servizio avviene su iniziativa dell'Amministrazione, che definisce di volta in volta l'ambito di intervento, gli obiettivi, le priorità e le modalità operative, anche nell'ambito dei Piani di Lavoro o di specifiche richieste operative. Il Fornitore opera esclusivamente su indicazione e previa autorizzazione dell'Amministrazione.

Il servizio è erogato in modalità di supporto tecnico-specialistico e affiancamento operativo alle strutture dell'Amministrazione e può essere attivato:

- su richiesta, in relazione a esigenze puntuali o non continuative;
- ad evento, in occasione di iniziative, progetti o interventi specifici.

Le attività possono essere svolte in modalità on-site presso le sedi dell'Amministrazione e/o da remoto, in funzione delle esigenze operative e secondo quanto di volta in volta concordato con l'Amministrazione.

Nell'erogazione del servizio, il Fornitore utilizza prioritariamente i processi, gli strumenti, le piattaforme e gli ambienti tecnologici messi a disposizione dall'Amministrazione. L'eventuale utilizzo di strumenti del Fornitore è ammesso esclusivamente alle condizioni previste dal Capitolato e previa autorizzazione dell'Amministrazione.

Il servizio non prevede presidi fissi, né attività di monitoraggio continuo, né servizi h24, e non si configura in alcun caso come servizio gestito o come assunzione di responsabilità end-to-end, che restano integralmente in capo all'Amministrazione.

Per tutte le attività gestite dal Fornitore nell'ambito del presente paragrafo, lo stesso dovrà condurre **SAL periodici settimanali** (o con diversa periodicità concordata con l'Amministrazione), e produrre la relativa documentazione in formato:

- **dettagliato** per le strutture operative;
- **executive** per le strutture direttive.

Inoltre, in caso di richieste di chiarimenti sull'operato da parte dell'Amministrazione, formalizzate attraverso i canali di comunicazione previsti o concordati nell'ambito del Contratto Esecutivo, il Fornitore dovrà fornire riscontro entro 2 giorni lavorativi.

2.6.2 Deliverable

Il presente paragrafo descrive i **deliverable minimi** che il Fornitore dovrà produrre nell'ambito del servizio di *Supporto Specialistico*, in coerenza con le attività descritte nel presente capitolo e con quanto definito nel Piano di Lavoro Generale e nei singoli Contratti Esecutivi.

I deliverable sono finalizzati a supportare l'Amministrazione nelle attività di governance, valutazione del rischio, prioritizzazione degli interventi e miglioramento continuo della postura di sicurezza.

ID	TITOLO	DESCRIZIONE	SLA
SS_1	Report di supporto specialistico	Documento tecnico che descrive le attività di supporto specialistico svolte, le analisi effettuate, le valutazioni prodotte e gli esiti delle attività di affiancamento operativo, in coerenza con l'ambito di intervento definito dall'Amministrazione.	Consegna entro 10 giorni lavorativi dalla conclusione delle attività di riferimento.
SS_2	Relazioni e documenti di analisi specialistica	Documenti di analisi tecnica e specialistica prodotti a supporto delle iniziative attivate, quali valutazioni, studi di fattibilità, analisi di impatto, analisi di rischio o approfondimenti tematici, redatti secondo le richieste dell'Amministrazione e nel rispetto del Piano di Lavoro.	Consegna entro i tempi definiti nel Piano di Lavoro Generale o nella specifica richiesta dell'Amministrazione.
SS_3	Piani e documentazione di supporto agli interventi	Documenti di pianificazione e supporto alle attività specialistiche, quali piani di intervento, piani di migrazione, piani di integrazione, piani di adeguamento o documentazione equivalente, prodotti a supporto delle attività richieste dall'Amministrazione.	Consegna entro i tempi definiti nel Piano di Lavoro Generale o nella specifica richiesta dell'Amministrazione.

ID	TITOLO	DESCRIZIONE	SLA
SS_4	Schemi e rappresentazioni tecniche	Schemi architetture, diagrammi, rappresentazioni tecniche o documentazione grafica a supporto delle attività di analisi, progettazione o affiancamento operativo svolte nell'ambito del servizio di Supporto specialistico.	Consegna entro i tempi definiti nel Piano di Lavoro Generale o nella specifica richiesta dell'Amministrazione.
SS_5	Report di security assessment AI/ML	Documento tecnico che descrive le componenti AI/ML analizzate, i principali rischi di sicurezza individuati e la loro contestualizzazione rispetto al contesto dell'Amministrazione.	Entro 20 giorni lavorativi dall'avvio delle attività di analisi, salvo diversa tempistica concordata nel Piano di Lavoro Generale.
SS_6	Mappe di esposizione delle componenti AI/ML	Rappresentazione delle superfici di esposizione e delle interazioni tra componenti AI/ML, servizi applicativi e infrastrutture in scope.	Contestuale al deliverable SS_5.
SS_7	Raccomandazioni tecniche di mitigazione	Documento contenente le misure tecniche e procedurali di mitigazione raccomandate, coerenti con i controlli di sicurezza adottati dall'Amministrazione.	Entro 5 giorni lavorativi dalla consegna del Report di security assessment AI/ML (SS_6).
SS_8	Contributo specialistico alle attività di Continuous Vulnerability Management	Evidenze tecniche e contributi specialistici finalizzati alla contestualizzazione dei risultati delle attività di Continuous Vulnerability Management, con riferimento a vulnerabilità, esposizioni e rischi che coinvolgono componenti o servizi basati su tecnologie di Intelligenza Artificiale e Machine Learning.	Entro 10 giorni lavorativi dalla disponibilità delle evidenze o dei risultati delle attività di Continuous Vulnerability Management di riferimento o diversa tempistica concordata nel Piano di Lavoro Generale.
SS_9	SAL periodico	Stato Avanzamento Lavori in formato operativo ed executive, comprensivo delle attività svolte nel periodo di riferimento.	Settimanale o mensile, secondo Piano di Lavoro
SS_10	Risposte a richieste di chiarimento	Riscontri tecnici a richieste di chiarimento dell'Amministrazione su attività o deliverable prodotti.	Entro 48 ore lavorative

L'Amministrazione valuterà i deliverable entro **5 giorni lavorativi** dalla consegna. In caso di richieste di modifica, il Fornitore dovrà aggiornare/modificare i deliverable entro **5 giorni lavorativi** dalla comunicazione della PA, salvo diversa tempistica concordata.

Tutte le tempistiche dovranno essere indicate nel Piano di Lavoro Generale.

Gli adempimenti indicati nel presente paragrafo e ad esso collegati sono valutati ai fini di rilievi/penali in:

- 4.1 IQ01 – *Rispetto di una scadenza contrattuale;*
- 4.2 IQ02 – *Adeguatezza delle figure professionali proposte per la erogazione dei servizi;*
- 4.5 IQ05 - *Turnover del personale impiegato nella fornitura;*
- 4.14 IQ14 – *Copertura del perimetro assegnato;*
- 4.18 IQ18 – *Completezza dei deliverable di Supporto specialistico;*
- 4.22 IQ22 – *Rilievi su obbligazioni contrattuali non presidiate.*

2.6.3 Figure professionali coinvolte

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 al capitolo 3 *Risorse da impiegare nell'esecuzione dei servizi*):

- Security Principal;
- Security Architect;
- Cloud Security Expert;
- OT/IoT Security Expert;
- Security Analyst;
- Security Specialist;
- Legal, Policy and Compliance Officer;
- Information Security Manager;
- AI Security Specialist;
- Security Engineer;
- Network Security Engineer.

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

2.6.4 Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento di tutti i servizi è: **Giorno/Persona**.

La modalità di remunerazione di tutti i servizi è: **a tempo/spesa oppure a corpo**.

In fase di offerta è richiesto al Concorrente di esprimere un prezzo per giorno/persona per ogni figura professionale prevista. I prezzi espressi saranno riferiti rispettivamente a:

- 8 ore lavorative complessive nella fascia oraria ferial Lun-Sab 8.00-20.00 (fascia standard).

In sede di Piano dei fabbisogni, l'Amministrazione definirà i deliverables richiesti e le risorse necessarie, indicando quindi il mix necessario per le attività richieste, in un'ottica di coerenza e proporzionalità.

2.7 Gestione accessi e identità

La **Gestione accessi e identità** è un ambito funzionale finalizzato a supportare l'Amministrazione nella progettazione e formalizzazione dei modelli operativi per la gestione degli accessi logici e delle identità digitali e, ove richiesto, nel supporto all'attuazione degli stessi, garantendo l'applicazione dei principi fondamentali di cybersicurezza quali il need to know, il least privilege e la segregation of duties (SoD).

I servizi attivabili nell'ambito si configurano come supporto tecnico-specialistico e operativo, erogato in affiancamento alle strutture dell'Amministrazione, ed è volto a supportare la definizione e l'implementazione di processi, regole e modelli organizzativi per il controllo degli accessi agli asset informativi, ai sistemi, alle applicazioni e alle infrastrutture dell'Amministrazione.

I servizi sono orientati a garantire che ogni utente, sistema o applicazione disponga esclusivamente dei privilegi strettamente necessari allo svolgimento delle proprie funzioni, assicurando la tracciabilità degli accessi, la corretta separazione dei compiti e la riduzione dei rischi connessi ad accessi non autorizzati, privilegi eccessivi o identità non correttamente gestite.

Rientrano, di conseguenza, le attività di supporto alla definizione e alla formalizzazione dei modelli operativi di gestione delle identità e degli accessi, nonché il supporto all'attuazione operativa dei processi di controllo, gestione e bonifica periodica dei profili, degli account e delle identità, finalizzata alla rimozione di account obsoleti, alla correzione dei privilegi non coerenti e all'eliminazione di identità duplicate o non più necessarie.

I servizi non si configurano come servizi gestiti, né come attività di governance o di controllo continuativo in autonomia da parte del Fornitore. Le responsabilità decisionali, di governo e di validazione finale dei modelli operativi e dei processi di gestione degli accessi restano integralmente in capo all'Amministrazione.

2.7.1 Attività previste

1. Formalizzazione dei modelli operativi per la gestione degli accessi e delle identità

Nell'ambito del servizio di Gestione accessi e identità, il Fornitore fornisce supporto tecnico-specialistico all'Amministrazione per la progettazione e la formalizzazione dei modelli operativi di gestione degli accessi e delle identità, finalizzati a garantire l'applicazione dei principi di need to know, least privilege e segregation of duties (SoD).

Le attività, svolte su indicazione e previa autorizzazione dell'Amministrazione, possono includere, a titolo esemplificativo e non esaustivo:

- analisi preliminare dei processi esistenti di gestione degli accessi e dei privilegi, con riferimento agli utenti, ai sistemi, alle applicazioni e alle identità digitali;
- supporto all'identificazione dei requisiti normativi, organizzativi e operativi applicabili alla gestione degli accessi e delle identità, in coerenza con il contesto dell'Amministrazione;
- supporto alla definizione dei modelli operativi di gestione degli accessi e delle identità basati sui principi di need to know, least privilege e segregation of duties;
- supporto alla formalizzazione di ruoli e responsabilità e alla mappatura degli accessi e dei privilegi associati a utenti, sistemi e applicazioni;
- supporto alla definizione e alla formalizzazione di policy, regole e procedure standardizzate per la gestione degli accessi e delle identità;
- supporto alla definizione delle modalità di verifica periodica dei modelli operativi e dei meccanismi di controllo degli accessi, inclusi gli aspetti di tracciabilità e auditabilità.

Le attività di formalizzazione dei modelli operativi non comportano l'assunzione di responsabilità decisionali o di governo dei processi, che restano integralmente in capo all'Amministrazione.

2. Attuazione operativa della gestione degli accessi logici

Nell'ambito del servizio di Gestione accessi e identità, il Fornitore può fornire supporto tecnico-specialistico e operativo all'attuazione dei modelli operativi definiti dall'Amministrazione, in relazione ai processi di gestione degli accessi logici e delle identità digitali.

Le attività, svolte sempre su indicazione e previa autorizzazione dell'Amministrazione, possono includere, a titolo esemplificativo e non esaustivo:

- supporto all'analisi preliminare degli asset critici e dei profili di accesso associati a utenti, sistemi e applicazioni;
- supporto alla configurazione e all'applicazione dei modelli di gestione degli accessi definiti dall'Amministrazione, inclusi i meccanismi di assegnazione, modifica e revoca dei privilegi;

- supporto all'implementazione e alla configurazione di strumenti e soluzioni di Identity and Access Management e di Identity Governance, ove adottati dall'Amministrazione, per l'attuazione dei modelli operativi definiti;
- supporto operativo alle attività di gestione delle richieste di accesso, di modifica e di revoca dei profili, secondo le regole e le procedure definite dall'Amministrazione;
- supporto alle attività di verifica periodica dei privilegi assegnati e alla bonifica dei profili, degli account e delle identità, finalizzata alla rimozione di account obsoleti, alla correzione dei privilegi non coerenti e all'eliminazione di identità duplicate o non più necessarie;
- supporto alle attività di monitoraggio degli accessi e di analisi delle anomalie, in coerenza con i processi e gli strumenti adottati dall'Amministrazione;
- supporto alle attività di integrazione dei processi di gestione degli accessi con altri processi e sistemi dell'Amministrazione;
- supporto alle attività di formazione e affiancamento operativo del personale dell'Amministrazione coinvolto nella gestione degli accessi e delle identità.

Le attività di attuazione operativa non si configurano come servizio gestito, né comportano presidi continuativi o assunzione di responsabilità end-to-end da parte del Fornitore.

Il servizio di Gestione accessi e identità è erogato secondo un modello flessibile e modulare, attivabile su richiesta dell'Amministrazione in funzione delle specifiche esigenze organizzative, operative o evolutive connesse alla gestione degli accessi logici e delle identità digitali.

Il servizio è erogato in affiancamento alle strutture dell'Amministrazione ed è articolato, in funzione delle esigenze espresse, in attività di supporto alla formalizzazione dei modelli operativi e in attività di supporto all'attuazione operativa dei processi di gestione degli accessi, secondo quanto definito dall'Amministrazione.

L'attivazione del servizio avviene su iniziativa dell'Amministrazione, che definisce di volta in volta l'ambito di intervento, le priorità, le modalità operative e gli obiettivi dell'intervento, anche nell'ambito di specifici Piani di Lavoro Generale o richieste operative. Il Fornitore opera esclusivamente su indicazione e previa autorizzazione dell'Amministrazione.

Le attività possono essere svolte in modalità on-site presso le sedi dell'Amministrazione e/o da remoto, in funzione delle esigenze operative e secondo quanto concordato con l'Amministrazione.

Il servizio non prevede presidi continuativi, né attività di gestione autonoma degli accessi o delle identità da parte del Fornitore e non si configura in alcun caso come servizio gestito. Le responsabilità di governo, validazione e decisione finale in materia di gestione degli accessi e delle identità restano integralmente in capo all'Amministrazione.

Per tutte le attività gestite dal Fornitore nell'ambito del presente paragrafo, lo stesso dovrà condurre **SAL periodici settimanali** (o con diversa periodicità concordata con l'Amministrazione), e produrre la relativa documentazione in formato:

- **dettagliato** per le strutture operative;
- **executive** per le strutture direttive.

Inoltre, in caso di richieste di chiarimenti sull'operato da parte dell'Amministrazione, formalizzate attraverso i canali di comunicazione previsti o concordati nell'ambito del Contratto Esecutivo, il Fornitore dovrà fornire riscontro entro 2 giorni lavorativi.

2.7.2 Deliverable

Il presente paragrafo descrive i **deliverable minimi** che il Fornitore dovrà produrre nell'ambito del servizio di *Gestione accessi e identità*, in coerenza con le attività descritte nel presente capitolo e con quanto definito nel Piano di Lavoro Generale e nei singoli Contratti Esecutivi.

I deliverable sono finalizzati a supportare l'Amministrazione nelle attività di governance, valutazione del rischio, prioritizzazione degli interventi e miglioramento continuo della postura di sicurezza.

ID	TITOLO	DESCRIZIONE	SLA
GA_1	Documento di modello operativo per la gestione degli accessi e delle identità	Documento che definisce il modello operativo di riferimento per la gestione degli accessi logici e delle identità digitali dell'Amministrazione, basato sui principi di need to know, least privilege e segregation of duties (SoD), costituendo il riferimento per la definizione delle policy e per l'attuazione operativa dei processi di gestione degli accessi.	Prima versione entro 15 giorni lavorativi dall'avvio delle attività di formalizzazione; eventuali aggiornamenti entro i tempi concordati nel Piano di Lavoro Generale.
GA_2	Policy e procedure per la gestione degli accessi e delle identità	Insieme di policy, regole e procedure standardizzate per la gestione degli accessi logici e delle identità digitali, incluse le modalità di assegnazione, modifica, revoca e verifica periodica dei privilegi, in coerenza con i modelli operativi definiti dall'Amministrazione.	Consegna entro i tempi definiti nel Piano di Lavoro Generale o nella specifica richiesta dell'Amministrazione.

ID	TITOLO	DESCRIZIONE	SLA
GA_3	Report di analisi e valutazione dei processi di gestione degli accessi	Documento di analisi dei processi esistenti di gestione degli accessi e delle identità, con evidenza delle valutazioni tecniche svolte e delle aree di miglioramento a supporto dell'adeguamento ai modelli operativi definiti dall'Amministrazione.	Consegna entro 10 giorni lavorativi dalla conclusione delle attività di analisi.
GA_4	Report di attuazione operativa e controllo degli accessi	Documento che descrive le attività di supporto all'attuazione operativa dei modelli di gestione degli accessi e delle identità, incluse le attività di gestione delle richieste di accesso, verifica dei privilegi e controllo delle identità, svolte in affiancamento all'Amministrazione.	Consegna con periodicità concordata nel Piano di Lavoro Generale o a conclusione delle attività di riferimento.
GA_5	Report di bonifica di profili, account e identità	Documento che descrive le attività di verifica e bonifica dei profili, degli account e delle identità digitali, finalizzate alla rimozione di account obsoleti, alla correzione dei privilegi non coerenti e all'eliminazione di identità duplicate o non più necessarie.	Consegna entro 10 giorni lavorativi dalla conclusione delle attività di bonifica o secondo quanto definito nel Piano di Lavoro Generale .
GA_6	SAL periodico	Stato Avanzamento Lavori in formato operativo ed executive , comprensivo delle attività svolte nel periodo di riferimento.	Settimanale o mensile , secondo Piano di Lavoro Generale
GA_7	Risposte a richieste di chiarimento	Riscontri tecnici a richieste di chiarimento dell'Amministrazione su attività o deliverable prodotti.	Entro 48 ore lavorative

L'Amministrazione valuterà i deliverable entro **5 giorni lavorativi** dalla consegna. In caso di richieste di modifica, il Fornitore dovrà aggiornare/modificare i deliverable entro **5 giorni lavorativi** dalla comunicazione della PA, salvo diversa tempistica concordata.

Tutte le tempistiche dovranno essere indicate nel Piano di Lavoro Generale.

Gli adempimenti indicati nel presente paragrafo e ad esso collegati sono valutati ai fini di rilievi/penali in:

- **4.1 IQ01 – Rispetto di una scadenza contrattuale;**

- 4.2 IQ02 – Adeguatezza delle figure professionali proposte per la erogazione dei servizi;
- 4.5 IQ05 - Turnover del personale impiegato nella fornitura;
- 4.6 IQ06 – Impegni assunti in offerta tecnica;
- 4.16 IQ16 – Conformità del modello di gestione delle identità (IAM);
- 4.17 IQ17 – Efficacia delle attività di bonifica IAM
- 4.22 IQ22 – Rilievi su obbligazioni contrattuali non presidiate.

2.7.3 Figure professionali coinvolte

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 al capitolo xx - Profili Professionali):

- Security Principal;
- Senior Security Consultant;
- Security Analyst;
- Security Specialist;
- Junior Security Consultant;
- Legal, Policy and Compliance Officer;
- Information Security Manager.

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

2.7.4 Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento di tutti i servizi è: **Giorno/Persona**.

La modalità di remunerazione di tutti i servizi è: **a tempo/spesa oppure a corpo**.

In fase di offerta è richiesto al Concorrente di esprimere un prezzo per giorno/persona per ogni figura professionale prevista. I prezzi espressi saranno riferiti rispettivamente a:

- 8 ore lavorative complessive nella fascia oraria ferial Lun-Sab 8.00-20.00 (fascia standard).

In sede di Piano dei fabbisogni, l'Amministrazione definirà i deliverables richiesti e le risorse necessarie, indicando quindi il mix necessario per le attività richieste, in un'ottica di coerenza e proporzionalità.

2.8 Formazione tecnica

Il servizio di Formazione tecnica è finalizzato al trasferimento strutturato di competenze operative al personale dell'Amministrazione, in coerenza con le specifiche esigenze formative e con le tecnologie in uso presso l'Amministrazione contraente.

Il servizio consente la fruizione di sessioni formative impartite presso le sedi dell'Amministrazione che permettano di istruire i discenti sulle specifiche tecnologie in ambito cybersicurezza indicate dall'Amministrazione, e deve avere l'obiettivo di:

- istruire i discenti sulle principali minacce che le tecnologie si prefiggono di contrastare;
- descrivere le tecnologie in termini di caratteristiche, configurazione e funzionalità, con particolare enfasi sulle componenti software;
- rendere il personale designato dall'Amministrazione Contraente in grado di provvedere alla gestione delle tecnologie in maniera autonoma ed ottimale;
- descrivere le eventuali attività di integrazione effettuate con altri prodotti presso l'Amministrazione e le relative finalità;
- realizzare demo e/o attività di test che consentano ai discenti di apprendere le principali funzionalità dei prodotti attraverso l'esperienza diretta.

È richiesto che tali attività formative siano erogate in moduli da massimo 24 ore e che per ogni modulo siano previsti al massimo 10 discenti. Ogni modulo è composto da due sezioni:

- una sezione teorica, in cui sono descritti i sistemi interessati e le relative funzionalità previste, indicativamente di 8 ore;
- una sezione pratica, in cui il personale dell'Amministrazione opererà attivamente sui sistemi, secondo una modalità *training on the job*, indicativamente di 16 ore.

Il numero dei moduli e, conseguentemente, la durata complessiva del servizio sarà concordata con l'Amministrazione sulla base dei sistemi richiesti, del grado di conoscenza dei discenti e del loro numero, e sarà riportata nel Piano di Lavoro Generale.

Il servizio di formazione tecnica e affiancamento dovrà essere svolto da personale dotato di conoscenza ed esperienza all'insegnamento dello specifico argomento, nel Piano di Lavoro Generale ne dovranno essere dettagliati programma, sessioni e durata complessiva, e in fase di presa in carico dovrà essere fornito il Curriculum vitae di ciascun docente previsto. L'organizzazione del corso sarà in ogni caso concordata con l'Amministrazione che avrà la facoltà di chiedere la sostituzione del docente in caso di non idoneità. Il personale proposto per le attività di formazione dovrà possedere i requisiti previsti al successivo paragrafo 3.2 per le figure di Security Analyst e/o Security Specialist, a seconda dell'esigenza dell'Amministrazione. Si applicano le previsioni sull'equivalenza di cui a tale paragrafo, fatta eccezione per i requisiti migliorativi offerti in AQ. I CV (e le eventuali certificazioni) dei docenti dovranno essere presentati entro i 15 giorni lavorativi

precedenti l'attivazione dei corsi di formazione. Sulla base dei CV presentati l'Amministrazione procederà alla verifica che il personale proposto sia in linea con i requisiti minimi, riservandosi la possibilità di procedere ad un colloquio di approfondimento per verificare la corrispondenza delle competenze elencate nel CV. Per il personale ritenuto inadeguato, qualunque sia il ruolo, l'Amministrazione Contraente procederà alla richiesta formale di sostituzione inviando apposita richiesta di sostituzione, in cui indicherà puntualmente la risorsa che ritiene inadeguata, le relative motivazioni in riferimento ai requisiti minimi e/o migliorativi di gara, la "data prevista di sostituzione" ai fini degli indicatori di qualità. La presentazione del CV (e delle eventuali certificazioni) della nuova risorsa in sostituzione dovrà quindi avvenire entro 5 giorni lavorativi.

I curriculum vitae delle figure professionali da impiegare dovranno essere resi disponibili alle Amministrazioni rispettando lo schema indicato al capitolo 5. Sarà facoltà dell'amministrazione indicare un diverso template. In ogni caso, dovranno essere particolarmente dettagliate le competenze ed esperienze tecniche al fine di verificare la corrispondenza con i requisiti minimi, gli eventuali requisiti migliorativi offerti e il contesto dell'Amministrazione.

Sulla base della complessità dei sistemi forniti e sulla base del grado di preparazione e conoscenza dei sistemi medesimi da parte del personale dell'Amministrazione che parteciperà al corso e a valle della presentazione del programma di addestramento da parte del Fornitore, l'Amministrazione potrà apportare opportune modifiche al programma di addestramento, presentato in fase preliminare, al fine di massimizzarne l'efficacia.

Le attività di formazione dovranno includere modalità strutturate di trasferimento delle competenze, anche mediante training-on-the-job e affiancamento operativo, finalizzate al consolidamento delle capacità tecniche interne all'Amministrazione.

Il Fornitore dovrà inoltre prevedere strumenti di valutazione dell'efficacia delle attività formative erogate e rendere disponibili i materiali didattici prodotti in formati idonei a consentirne il riuso interno e l'aggiornamento da parte dell'Amministrazione.

I materiali formativi dovranno essere accompagnati da condizioni d'uso che ne consentano il riutilizzo da parte dell'Amministrazione.

Sarà a carico del Fornitore la predisposizione di una scheda di valutazione:

- che rispecchi gli argomenti riportati nel programma del corso di addestramento specifico e consenta una valutazione del grado di apprendimento;
- preveda una valutazione del trattamento degli stessi da parte del personale dell'Amministrazione partecipante al corso con tre livelli di gradimento, di cui uno insufficiente.

Al termine di ciascuna sessione:

- i discenti che non abbiano raggiunto un livello sufficiente dovranno essere oggetto di una ulteriore sessione formativa per colmare il gap riscontrato;
- l'Amministrazione valuterà le schede compilate dai partecipanti e, in caso di una valutazione negativa da parte di almeno il 30% dei partecipanti, dovrà essere ripetuta la sessione per gli argomenti che hanno avuto gradimento negativo.

In seguito alla valutazione positiva effettuata dall'Amministrazione, a conclusione del corso l'Aggiudicatario rilascerà:

- all'Amministrazione un *Verbale di erogazione del Corso* attestante la data di effettiva erogazione del servizio, la durata, il programma seguito ed eventuali criticità emerse;
- ai discenti un attestato, o analogo documento, che dimostri il conseguimento degli obiettivi.

Le date di erogazione del servizio in oggetto e il programma dovranno essere preventivamente previste e concordate nel Piano di Lavoro Generale.

L'erogazione del servizio dovrà essere garantita dalla data di approvazione del Piano di Lavoro Generale e fino alla scadenza del Contratto Esecutivo (anche eventualmente prorogata nei casi previsti dall'Accordo Quadro e comunque dalla normativa vigente), secondo quanto riportato nel Piano di Lavoro Generale.

Gli adempimenti indicati nel presente paragrafo sono valutati ai fini di rilievi/penali in:

- 4.1 IQ01 – *Rispetto di una scadenza contrattuale;*
- 4.2 IQ02 – *Adeguatezza delle figure professionali proposte per la erogazione dei servizi;*
- 4.5 IQ05 - *Turnover del personale impiegato nella fornitura;*
- 4.6 IQ06 – *Impegni assunti in offerta tecnica.*
- 4.19 IQ19 – *Erogazione dei moduli di formazione tecnica;*
- 4.20 IQ20 – *Efficacia della formazione tecnica;*
- 4.21 IQ21 – *Conformità dei docenti e della documentazione formativa*
- 4.22 IQ22 – *Rilievi su obbligazioni contrattuali non presidiate.*

2.8.1 **Metrica di dimensionamento e modalità di remunerazione**

La metrica di dimensionamento è: **modulo formativo erogato.**

La modalità di remunerazione è: **a consumo per singolo modulo.**

3 RISORSE DA IMPIEGARE NELL'ESECUZIONE DEI SERVIZI

Con riferimento a ciascuno dei servizi oggetto dei Lotti 1 e 2, tutte le risorse che il Fornitore impiegherà per l'erogazione dei servizi oggetto della fornitura dovranno essere adeguate al ruolo ricoperto e dovranno essere in possesso almeno dei requisiti minimi espressi dal presente Capitolato Tecnico Speciale, integrati con tutte le migliorie eventualmente indicate in Offerta Tecnica.

Nel Piano dei Fabbisogni la singola Amministrazione specificherà nel dettaglio le proprie esigenze, indicando le figure professionali richieste per ciascun servizio, tra quelle indicate nel seguito, e la rispettiva quantità espressa in giorni persona. È facoltà dell'Amministrazione, in sede di Piano dei Fabbisogni, dettagliare le proprie esigenze precisando le competenze ed esperienze tra quelle indicate per ciascun profilo nell'ambito delle tabelle di seguito riportate. A tal fine, per ciascun profilo professionale le competenze ed esperienze indicate nelle tabelle di cui al presente paragrafo devono essere presenti nel complesso delle risorse professionali che il Fornitore metterà a disposizione dell'Amministrazione per l'erogazione dei servizi e **NON** devono essere interamente possedute da un'unica risorsa. Resta inteso che, al contrario, i titoli di studio (o la cultura equivalente), l'anzianità lavorativa e le certificazioni dovranno essere posseduti da ciascuna risorsa. In ogni caso, fermo restando quanto sopra, l'Amministrazione può richiedere, nell'ambito di ogni specifico profilo, più risorse distinte, specializzate ciascuna in un determinato ambito tecnologico.

Con riferimento alle certificazioni:

- per le certificazioni migliorative eventualmente offerte, resta fermo quanto indicato in offerta tecnica;
- tutte le certificazioni possedute dalle risorse per ciascun ruolo dovranno essere mantenute aggiornate e in corso di validità per tutta la durata contrattuale.

Inoltre, il Piano dei Fabbisogni dell'Amministrazione sarà corredato dalla descrizione del contesto tecnologico attuale e futuro di riferimento.

Nell'ambito del Piano Operativo predisposto dal Fornitore, saranno declinati i profili professionali in coerenza con il suddetto contesto descritto dall'Amministrazione. Permane in ogni caso l'obbligo per il Fornitore di erogare i servizi richiesti anche a fronte di significative variazioni del suddetto contesto tecnologico, adeguando le conoscenze del personale impiegato nell'erogazione dei servizi o inserendo nei gruppi di lavoro risorse con skill adeguato, fermo restando quanto previsto nel presente documento.

Ciascun profilo professionale si riferisce a risorse professionali con ampia esperienza, competenza funzionale e tecnica per l'ambito del Lotto e non ad una singola persona. Tali competenze dovranno essere costantemente aggiornate all'evoluzione della tecnologia e della normativa di riferimento, nonché degli standard, delle linee guida e best practices applicabili.

Nel presente documento, e laddove citati nel Capitolato Tecnico Generale, ogni riferimento ad attività o metodologie basate sull'adozione di prodotti e ogni riferimento a prodotti vanno intesi in relazione ai prodotti e/o ai componenti di tali prodotti che sono effettivamente adottati per i sistemi informatici gestiti dalla singola Amministrazione.

Le competenze ed esperienze delle figure che seguono non sono esaustive delle esigenze future. Infatti, le competenze ed esperienze iniziali potranno variare in funzione dell'evoluzione tecnologica, normativa e in relazione a ulteriori tematiche, prodotti, sistemi e metodologie che emergeranno durante la validità dell'Accordo Quadro e dei Contratti Esecutivi. A tal fine, le sottostanti tabelle potranno essere aggiornate nel corso della vigenza dell'Accordo Quadro e dei Contratti Esecutivi, in accordo tra Consip e il Fornitore.

Per ogni profilo è richiesto il possesso di una anzianità lavorativa minima, che deve essere stata maturata in ambito ICT. Per ogni profilo è richiesto inoltre il possesso di uno specifico titolo di studio oppure di una "cultura equivalente".

La cultura equivalente corrisponde ad una anzianità lavorativa maturata in ambito ICT aggiuntiva rispetto a quella minima indicata nel profilo stesso; l'entità dell'esperienza aggiuntiva necessaria dipende dal titolo di studio posseduto dalla risorsa rispetto a quello richiesto, come indicato nella sottostante tabella.

In ogni caso, il titolo di studio posseduto deve essere almeno un diploma di scuola secondaria di secondo grado.

TITOLO DI STUDIO POSSEDUTO TITOLO DI STUDIO RICHIESTO	LAUREA MAGISTRALE IN DISCIPLINE TECNICO SCIENTIFICHE	LAUREA TRIENNALE IN DISCIPLINE TECNICO SCIENTIFICHE	LAUREA MAGISTRALE (ALTRE DISCIPLINE)	LAUREA TRIENNALE (ALTRE DISCIPLINE)	DIPLOMA DI PERITO TECNICO INDUSTRIALE IN INFORMATICA	DIPLOMA DI SCUOLA SECONDARIA DI SECONDO GRADO (DIVERSO DA PERITO TECNICO INDUSTRIALE IN INFORMATICA)
LAUREA MAGISTRALE IN DISCIPLINE TECNICO SCIENTIFICHE	-	+ 2 anni	+ 2 anni (o master 2° livello in cybersecurity)	+ 3 anni (o + 2 anni e master 1° livello in cybersecurity)	+ 5 anni	+ 7 anni
LAUREA TRIENNALE IN DISCIPLINE TECNICO SCIENTIFICHE	-	-	+ 1 anno (o master 1° livello in cybersecurity)	+ 2 anni (o + 1 anno e master 1° livello in cybersecurity)	+ 4 anni	+ 5 anni

Tabella 1. Esperienza aggiuntiva da considerare come “cultura equivalente”

Ad esempio, nel caso in cui fosse richiesta una laurea magistrale in discipline tecnico-scientifiche con esperienza minima di 10 anni, il possesso di laurea triennale in discipline tecnico-scientifiche richiederebbe esperienza minima di 12 anni (10 + 2).

Si precisa che per lauree in discipline scientifiche si intendono le lauree che possono essere ricondotte alle classi di laurea che prevedono, nelle proprie attività formative di base e/o caratterizzanti, uno o più dei settori scientifico disciplinari inclusi nelle aree “scienze matematiche e tecnologie informatiche” o “informatica” o “ingegneria dell'informazione (telecomunicazioni, informatica)” o “sicurezza informatica”.

Le classi di laurea e i settori scientifico-disciplinari suddetti fanno riferimento alla classificazione fornita dal Ministero dell'Istruzione, Università e Ricerca nell'ambito dei D.M. 16 marzo 2007 e s.m.i. e 4 ottobre 2000 e s.m.i., nonché secondo quanto previsto dai D.M. 1648 e 1649 del 19 dicembre 2023.

L'eventuale equiparazione dei diplomi di laurea conseguiti in base ad ordinamenti previgenti è regolata da quanto previsto nel Decreto Interministeriale 9 luglio 2009 (G.U. 7 ottobre 2009 n. 233) e s.m.i.

3.1.1 Security Principal

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale senior responsabile del governo tecnico e operativo delle attività di cybersecurity erogate nell'ambito dei servizi previsti dal Capitolato, con funzioni di coordinamento, indirizzo e controllo della qualità delle attività svolte dal team del Fornitore, in raccordo con l'Amministrazione.
Missione e ambito di intervento	Opera come punto di riferimento tecnico strategico per l'Amministrazione, assicurando la corretta pianificazione, esecuzione e supervisione delle attività di sicurezza informatica previste dai servizi del Capitolato, incluse quelle di governance, supporto specialistico, sicurezza dei sistemi e delle applicazioni, gestione degli incidenti, gestione delle identità e supporto all'evoluzione architetturale. La figura non assume responsabilità di gestione diretta dei sistemi dell'Amministrazione , ma svolge un ruolo di indirizzo, coordinamento e validazione tecnica, garantendo la coerenza delle attività con il Piano di Lavoro Generale, con le normative applicabili e con le best practice di settore.
Competenze ed esperienze richieste	Il Security Principal deve possedere comprovata esperienza in ambito cybersecurity, maturata in contesti complessi, e in particolare: – coordinamento tecnico di servizi e progetti di cybersecurity, privacy e continuità operativa in ambito ICT complesso e multi-dominio; – capacità di interlocuzione tecnica e manageriale con i referenti dell'Amministrazione, inclusi responsabili IT, responsabili della sicurezza, strutture di governance e controllo; – definizione e supervisione di modelli di sicurezza, processi, policy e procedure in coerenza con standard e framework di riferimento; – conoscenza del quadro normativo nazionale ed europeo in materia di sicurezza informatica e continuità operativa, protezione dei dati e cybersicurezza della Pubblica Amministrazione; – conoscenza dei principali standard, framework e linee guida in materia di sicurezza delle informazioni, cybersecurity, continuità operativa e service management, quali, a titolo esemplificativo: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, ITIL, COBIT, CMMI, NIST, nonché

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	delle relative modalità di applicazione nel contesto della Pubblica Amministrazione; – conoscenza delle metodologie di program e project management applicate alla pianificazione, al coordinamento e al controllo di servizi e progetti di cybersecurity complessi e delle principali certificazioni tra PRINCE2 Practitioner, PgMP, PMP, UNI 11648 o equivalenti; – governo e controllo delle attività di: - o incident management e supporto alla gestione degli eventi di sicurezza; - o vulnerability management, penetration test e analisi della postura di sicurezza; - o sicurezza dei sistemi, delle applicazioni e delle infrastrutture; - o supporto specialistico e progettazione di soluzioni di cybersecurity; – supervisione della qualità e della completezza dei deliverable prodotti, inclusi report tecnici, documentazione di analisi e SAL; – esperienza nella gestione di team multidisciplinari e nel coordinamento di figure professionali senior e junior.
Certificazioni	È richiesto il possesso di almeno una certificazione in ambito cybersecurity o governance della sicurezza, tra: – CISSP – Certified Information Systems Security Professional; – CISM – Certified Information Security Manager; – CISA – Certified Information Systems Auditor; – CRISC – Certified in Risk and Information Systems Control; Le certificazioni devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea magistrale in discipline tecnico scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 10 anni in ambito ICT, di cui almeno 5 anni in ruoli riconducibili alla cybersecurity, alla sicurezza delle informazioni o alla governance della sicurezza.

3.1.2 Security Architect

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale senior responsabile della progettazione, revisione e validazione delle architetture di sicurezza dei sistemi informativi dell'Amministrazione, in coerenza con i requisiti di cybersecurity, resilienza, integrazione tecnologica e compliance previsti dal Capitolato.
Missione e ambito di intervento	Il Security Architect supporta l'Amministrazione nella definizione e nell'evoluzione delle architetture di sicurezza a livello infrastrutturale, applicativo e di integrazione, assicurando l'adozione dei principi di <i>security by design</i> e <i>security by default</i> . Opera nell'ambito dei servizi previsti dal Capitolato, in particolare nelle attività di supporto specialistico, sicurezza dei sistemi e delle applicazioni, gestione delle identità e supporto all'evoluzione architetturale, senza assumere responsabilità di gestione operativa diretta dei sistemi.
Competenze ed esperienze richieste	Il Security Architect deve possedere comprovata esperienza nella progettazione di soluzioni di cybersecurity in contesti ICT complessi e, in particolare: – progettazione e revisione di architetture di sicurezza per ambienti on-premise, cloud e ibridi; – definizione di modelli architetturali di sicurezza per infrastrutture, applicazioni e servizi digitali; – integrazione di soluzioni di sicurezza (es. sistemi di protezione perimetrale, soluzioni di monitoraggio e detection, Identity & Access Management); – analisi dei requisiti di sicurezza e traduzione degli stessi in requisiti architetturali e tecnici;

VOCE	DESCRIZIONE
	– valutazione dei rischi architetturali e delle misure di mitigazione; – capacità di analisi delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza; – capacità di comprendere infrastrutture ICT complesse e le relazioni tra i differenti sistemi e componenti infrastrutturali; – conoscenza delle problematiche di sicurezza delle infrastrutture ICT e dei contesti IT/OT; – conoscenza delle metodologie e degli strumenti per la verifica dell'efficacia delle contromisure di sicurezza; – conoscenza delle principali tecnologie di sicurezza ICT, incluse soluzioni cloud e SaaS, minacce di nuova generazione e modalità di contenimento; – conoscenza dei sistemi di monitoraggio e correlazione degli eventi di sicurezza e delle logiche di integrazione; – conoscenza dei principi e dei sistemi di Identity & Access Management, data classification e gestione delle identità digitali; – esperienza nell'analisi architetturale di infrastrutture ICT finalizzata all'individuazione di criticità di sicurezza; – esperienza nella definizione di soluzioni tecnologiche e organizzative per il miglioramento della postura di sicurezza; – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo e con i team tecnici dell'Amministrazione per garantire coerenza architetturale e aderenza ai requisiti di sicurezza.
Certificazioni	Possesso di almeno una certificazione in ambito architetture di sicurezza o cybersecurity, tra cui, a titolo esemplificativo e non esaustivo: – CISSP (Certified Information Systems Security Professional), in ambito progettazione e governo della sicurezza delle informazioni; – CISSP-ISSAP (Information Systems Security Architecture Professional), in ambito architetture di sicurezza; – CCSP (Certified Cloud Security Professional), in ambito sicurezza delle architetture cloud;

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	– CompTIA CySA+, in ambito analisi e progettazione di soluzioni di sicurezza e gestione delle minacce; per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo. Le certificazioni devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea magistrale in discipline tecnico scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 8 (otto) anni nel settore ICT, di cui almeno 4 (quattro) maturati in attività riconducibili alla progettazione di architetture di sicurezza o alla cybersecurity.

3.1.3 Cloud Security Expert

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale specializzata nella sicurezza degli ambienti cloud , responsabile della progettazione, configurazione e gestione delle misure di sicurezza a protezione di infrastrutture, piattaforme e servizi cloud.
Missione e ambito di intervento	Opera nell'ambito dei servizi previsti dal Capitolato con riferimento alla sicurezza degli ambienti cloud , supportando l'Amministrazione nella protezione delle risorse cloud e dei dati, nella configurazione sicura dei servizi e nel rispetto dei requisiti di sicurezza e compliance applicabili agli ambienti cloud pubblici, privati o ibridi.
Competenze ed esperienze richieste	Il Cloud Security Expert deve possedere comprovata esperienza in contesti ICT complessi e, in particolare: – progettazione e implementazione di misure di sicurezza per ambienti cloud (IaaS, PaaS, SaaS); – configurazione sicura di servizi cloud, incluse reti, identità, accessi e logging; – gestione di Identity and Access Management (IAM) in contesti cloud;

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	– implementazione di controlli di sicurezza per la protezione dei dati e delle comunicazioni; – supporto alle attività di hardening degli ambienti cloud; – analisi delle configurazioni cloud e individuazione di vulnerabilità o misconfigurazioni; – integrazione degli ambienti cloud con sistemi di monitoraggio e sicurezza; – supporto tecnico alle attività di gestione degli eventi di sicurezza che coinvolgono ambienti cloud; – redazione di documentazione tecnica relativa alle architetture e alle configurazioni di sicurezza cloud; – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo.
Certificazioni	Possesso di almeno una delle seguenti certificazioni: – CompTIA Cloud+ (Computing Technology Industry Association – Cloud Plus); – CCSP – Certified Cloud Security Professional (ISC² – International Information System Security Certification Consortium); – AWS Certified Security – Specialty (Amazon Web Services); – Microsoft Certified: Azure Security Engineer Associate (Microsoft); – Google Professional Cloud Security Engineer (Google Cloud Platform); per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo. Le certificazioni devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea triennale o magistrale in discipline tecnico-scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 5 (cinque) anni in ambito ICT, di cui almeno 3 (tre) maturati in attività di sicurezza cloud o sicurezza delle infrastrutture cloud.

3.1.4 OT/IoT Security Expert

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale specializzata nella sicurezza di ambienti Operational Technology (OT) e Internet of Things (IoT) , responsabile della progettazione e dell'implementazione dei controlli di sicurezza, della configurazione sicura di reti e apparati industriali, nonché del supporto tecnico alle attività di monitoraggio, valutazione e miglioramento della postura di sicurezza in contesti ICS/SCADA e IoT.
Missione e ambito di intervento	Opera nell'ambito dei servizi previsti dal Capitolato con riferimento alla sicurezza dei sistemi e delle reti OT/IoT , contribuendo alla definizione e applicazione delle misure tecniche di protezione, alla segmentazione e al controllo dei flussi tra domini IT/OT, alla gestione sicura degli accessi e alla verifica della conformità agli standard e alle linee guida applicabili nei contesti industriali e IoT.
Competenze ed esperienze richieste	L'OT/IoT Security Expert deve possedere comprovata esperienza in contesti complessi e, in particolare: – progettazione e implementazione di architetture di sicurezza per sistemi OT/IoT (es. ICS/SCADA, DCS, PLC, RTU, HMI), incluse segmentazione di rete, gestione delle zone e conduits, controllo dei flussi IT/OT; – configurazione sicura di componenti e apparati (gateway, controller, asset IoT, sistemi di telemetria) e delle interfacce di comunicazione industriale; – conoscenza e gestione dei protocolli OT/IoT (ad es. Modbus, DNP3, IEC-61850, OPC/OPC-UA, PROFINET) e dei relativi rischi/contromisure; – hardening degli ambienti OT/IoT e applicazione di controlli compensativi in presenza di vincoli di disponibilità/sicurezza funzionale; – valutazione delle vulnerabilità e verifica delle misconfigurazioni su apparati OT/IoT, con attenzione a impatti su safety, disponibilità e continuità operativa; – integrazione con sistemi di monitoraggio e di rilevazione delle minacce (es. network sensors OT, log di apparati, piattaforme di asset inventory/asset discovery per OT/IoT);

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	– gestione sicura degli accessi remoti agli ambienti OT/IoT (ad esempio tramite jump server e meccanismi di controllo degli accessi), garantendo la tracciabilità delle sessioni di manutenzione e delle attività svolte da fornitori e terze parti; – documentazione tecnica (architetture, configurazioni, piani di segregazione/segmentazione, linee guida operative) e supporto alle verifiche/audit; – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo.
Certificazioni	Possesso di almeno una delle seguenti certificazioni: – GICSP – Global Industrial Cyber Security Professional (GIAC); – CSSA – Certified SCADA Security Architect (IACRB – Information Assurance Certification Review Board); – CISSP – Certified Information Systems Security Professional ((ISC)² – International Information System Security Certification Consortium); – CISM – Certified Information Security Manager (ISACA – Information Systems Audit and Control Association); – SC-200 – Microsoft Security Operations Analyst (Microsoft); – CompTIA Security+ (Computing Technology Industry Association); per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo. Le certificazioni devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea magistrale in discipline tecnico-scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 5 (cinque) anni in ambito ICT/OT, di cui almeno 3 (tre) maturati in sicurezza OT/IoT o in contesti ICS/SCADA/IIoT con responsabilità diretta di progettazione/implementazione dei controlli di sicurezza.

3.1.5 Senior Security Consultant

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale senior che fornisce supporto consulenziale e tecnico-specialistico avanzato nell'ambito della cybersecurity e della sicurezza delle informazioni, supportando l'Amministrazione nelle attività di analisi, valutazione, indirizzo e miglioramento della postura di sicurezza, in coerenza con i servizi previsti dal Capitolato.
Missione e ambito di intervento	Opera nell'ambito dei servizi previsti dal Capitolato svolgendo un ruolo di consulenza senior e di raccordo tecnico tra le esigenze dell'Amministrazione, le figure di governo della sicurezza e i team operativi, contribuendo alla corretta applicazione dei modelli di sicurezza, dei processi e delle misure tecniche adottate. La figura supporta l'Amministrazione nelle attività di valutazione e gestione del rischio cyber, nella protezione dei sistemi e delle applicazioni e nella gestione delle identità e degli accessi, assicurando coerenza con il quadro normativo, gli standard di riferimento e le best practice di settore.
Competenze ed esperienze richieste	Il Senior Security Consultant deve possedere consolidata esperienza in contesti ICT complessi e, in particolare, è in grado di: – fornire supporto consulenziale avanzato nell'ambito della gestione del rischio cyber, della valutazione della security posture e dell'individuazione delle priorità di intervento; – contribuire alle attività di Continuous Vulnerability Management, supportando l'interpretazione e la correlazione dei risultati delle attività di vulnerability assessment e penetration test e indirizzando le azioni di remediation in coerenza con il contesto operativo e di rischio; – supportare le attività di sicurezza dei sistemi e delle applicazioni, contribuendo all'indirizzo delle attività di hardening, patching e verifica della sicurezza applicativa, nonché alla valutazione delle evidenze tecniche e alla definizione delle azioni correttive; – supportare le attività di gestione delle identità e degli accessi, contribuendo alla definizione, verifica e valutazione dei modelli operativi di controllo degli accessi, dei meccanismi di segregazione dei ruoli e dei principi di sicurezza adottati;

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	– collaborare alla definizione e all'aggiornamento di processi, procedure e linee guida in ambito sicurezza delle informazioni, cybersecurity e privacy, in coerenza con gli standard e i framework di riferimento; – possedere buona conoscenza dei processi ICT e delle metodologie di gestione dei progetti, contribuendo al coordinamento delle attività e al supporto delle risorse junior coinvolte nei servizi; – fornire supporto alle attività di continuità operativa e gestione degli eventi di sicurezza, contribuendo all'analisi degli impatti, alla valutazione delle misure adottate e alla gestione delle azioni correttive; – redigere documentazione tecnica e consulenziale, report di analisi, valutazioni di sicurezza e contributi a supporto dei processi decisionali dell'Amministrazione; – collaborare con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, garantendo coerenza tecnica, qualità delle attività e allineamento agli indirizzi definiti.
Certificazioni	Possesso di almeno una delle seguenti certificazioni, aggiornate all'ultima release disponibile: – Certified Information Security Manager (CISM); – Certified Information Systems Security Professional (CISSP); – Certified Ethical Hacker (CEH); – Certified Information Systems Auditor (CISA); – Certified Information Privacy Professional (CIPP); – CompTIA Security+; – Lead Auditor ISO/IEC 27001. per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun Contratto Esecutivo. Le certificazioni, se possedute, devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea magistrale in discipline tecnico-scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Anzianità lavorativa di almeno 7 (sette) anni nel settore ICT, di cui almeno 4 (quattro) anni di provata esperienza nella specifica funzione,

3.1.6 Forensics Expert

VOCE	DESCRIZIONE
Descrizione sintetica	Figura operativa specializzata nel reperimento, preservazione, analisi e presentazione di evidenze digitali a supporto delle indagini forensi informatiche e delle attività di accertamento tecnico, nel rispetto di procedure e metodologie riconosciute.
Missione e ambito di intervento	Opera nell'ambito dei servizi previsti dal Capitolato con riferimento alle attività di digital forensics. In particolare, cura la corretta acquisizione e conservazione delle evidenze, l'analisi tecnica dei supporti e dei sistemi coinvolti, la documentazione delle attività e la produzione dei risultati in forma utilizzabile nei procedimenti interni ed esterni all'Amministrazione. <i>Perimetro:</i> la figura svolge attività forensi (acquisizione, preservazione, analisi, reporting). Le attività di gestione operativa dell'incidente (contenimento, eradicazione, ripristino) sono in carico ad alte figure quali l'Incident Responder.
Competenze ed esperienze richieste	Il Forensics Expert deve possedere comprovata esperienza in contesti ICT complessi e, in particolare: – acquisizione forense di dati e artefatti digitali da sistemi, endpoint, dispositivi mobili e ambienti virtualizzati/cloud, con preservazione dell'integrità e tracciabilità della catena di custodia; – analisi forense su immagini e supporti digitali (file system, registry, log, artefatti di sistema, e-mail, browser, applicazioni), inclusa timeline analysis e correlazione eventi; – utilizzo di strumenti e toolkit forensi per acquisizione, parsing, triage e reporting; – redazione di rapporti tecnici forensi completi, riproducibili e verificabili, con allegazione di evidenze; – collaborazione con i referenti dell'Amministrazione per le richieste interne e, ove previsto, supporto tecnico verso Autorità e terze parti; – aggiornamento continuo su metodologie, standard e best practice di digital forensics; – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo.

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
Certificazioni	Possesso di almeno una delle seguenti certificazioni: – GIAC Certified Forensic Examiner (GCFE); – GIAC Certified Forensic Analyst (GCFA); – Certified Cyber Forensics Professional (CCFP); per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun Contratto Esecutivo. Le certificazioni devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea magistrale in discipline tecnico-scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 8 (otto) anni in ambito ICT, di cui almeno 3 (tre) maturati in digital forensics o attività strettamente riconducibili (acquisizione/preservazione evidenze, analisi forense, reporting forense).

3.1.7 Security Analyst

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale specializzata nelle attività di analisi tecnica degli eventi e delle condizioni di sicurezza dei sistemi informativi dell'Amministrazione, a supporto dei servizi di cybersecurity previsti dal Capitolato.
Missione e ambito di intervento	Il Security Analyst supporta l'Amministrazione nelle attività di analisi degli eventi di sicurezza, delle vulnerabilità e della postura complessiva dei sistemi, contribuendo all'identificazione delle minacce, alla valutazione dei rischi e alla produzione delle evidenze tecniche a supporto delle decisioni operative e di governo. Opera nell'ambito dei servizi previsti dal Capitolato, in particolare nei servizi di incident management, continuous vulnerability management, sicurezza dei sistemi e delle applicazioni e conduzione operativa, svolgendo attività di analisi e supporto specialistico.
Competenze ed esperienze richieste	Il Security Analyst deve possedere comprovata esperienza nell'analisi tecnica della sicurezza in contesti ICT complessi e, in particolare:

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	– analisi e classificazione degli eventi di sicurezza e degli alert generati dai sistemi di monitoraggio e correlazione; – analisi delle vulnerabilità e supporto alla valutazione della postura di sicurezza di infrastrutture, applicazioni e servizi; – capacità di interpretazione dei risultati di vulnerability assessment e penetration test; – conoscenza delle principali minacce informatiche e delle tecniche di attacco; – capacità di coordinamento operativo di risorse junior nell'ambito delle attività di analisi della sicurezza; – conoscenza dei processi e delle procedure operative ICT; – conoscenza dei processi di incident handling ed escalation per la gestione degli incidenti di sicurezza informatica; – esperienza nella definizione e nell'analisi di configurazioni di sicurezza; – esperienza nella definizione di regole di correlazione e nel tuning delle stesse; – supporto alla produzione di report tecnici, documentazione di analisi e SAL; – collaborazione con il Security Architect, l'Incident Responder e il Security Principal per la gestione coordinata delle attività di sicurezza. – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo.
Certificazioni	Non previsto
Titolo di studio	Laurea magistrale in discipline tecnico scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore ad almeno 6 (sei) anni nel settore ICT, di cui almeno 4 (quattro) anni maturati in attività riconducibili alla cybersecurity o all'analisi della sicurezza delle informazioni.

3.1.8 Security Specialist

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale trasversale che supporta operativamente l'erogazione dei servizi di cybersecurity previsti dal Capitolato, contribuendo all'applicazione delle misure di sicurezza, alla verifica delle configurazioni, al supporto alle attività tecniche sui diversi ambiti di servizio e alla produzione della documentazione tecnica a supporto delle attività.
Missione e ambito di intervento	Opera nell'ambito dei servizi previsti dal Capitolato con riferimento alle attività operative di sicurezza delle informazioni (ad es. supporto a sicurezza dei sistemi e delle applicazioni, gestione delle configurazioni, monitoraggio tecnico e reporting), in coerenza con le architetture e le politiche di sicurezza definite dall'Amministrazione e dalle figure di governo/architettura.
Competenze ed esperienze richieste	Il Security Specialist deve possedere esperienza in contesti ICT complessi e articolati e adeguate competenze tecnico-operative, maturate nel supporto trasversale all'erogazione dei servizi di cybersecurity previsti dal Capitolato. In particolare, il profilo è in grado di: – supportare operativamente le attività di Asset Inventory e Asset Management, contribuendo alla rilevazione, classificazione e aggiornamento delle informazioni sugli asset ICT, nonché alla loro integrazione con i sistemi di gestione dei servizi e di sicurezza, assicurando coerenza, accuratezza e tracciabilità dei dati; – contribuire alle attività di presidio operativo della sicurezza e di gestione degli eventi e degli incidenti di sicurezza, attraverso il monitoraggio delle piattaforme di sicurezza, l'analisi e la gestione degli alert, la gestione dei ticket e il supporto alle attività di escalation, nel rispetto delle procedure e dei playbook definiti; – fornire supporto alle attività di Continuous Vulnerability Management, collaborando alla conduzione delle analisi di vulnerabilità, all'integrazione e correlazione dei risultati provenienti da fonti diverse, alla valutazione della postura di sicurezza e al supporto alle attività di remediation e verifica degli interventi correttivi; – supportare l'implementazione e il mantenimento delle misure di sicurezza per sistemi e applicazioni, incluse le attività di hardening, patching e supporto operativo alle verifiche di sicurezza applicativa, contribuendo alla raccolta delle evidenze tecniche e alla documentazione delle attività svolte; – operare nell'ambito delle attività di conduzione, contribuendo alla gestione operativa delle soluzioni di sicurezza e degli apparati

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	tecnologici, alla verifica delle configurazioni, all'applicazione delle politiche definite e alla produzione della reportistica tecnica prevista; – supportare l'attuazione operativa dei processi di gestione delle identità e degli accessi, collaborando all'esecuzione delle attività di provisioning, revisione e bonifica degli accessi, al monitoraggio delle autorizzazioni e alla verifica del rispetto dei principi di sicurezza definiti; – fornire supporto alle attività di supporto specialistico, contribuendo alle iniziative di integrazione e migrazione tecnologica e all'adeguamento delle soluzioni di sicurezza, in coerenza con le architetture e gli indirizzi definiti dalle figure di governo e di progettazione; – partecipare alle attività di formazione tecnica previste dal Capitolato, con particolare riferimento alla componente pratica e laboratoriale, a supporto del trasferimento delle competenze operative sull'utilizzo degli strumenti e delle soluzioni di sicurezza; – collaborare con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività, la coerenza operativa e il rispetto delle modalità organizzative previste.
Certificazioni	Non richieste
Titolo di studio	Laurea triennale o magistrale in discipline tecnico-scientifiche, oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 3 (tre) anni in ambito ICT, di cui almeno 2 (due) maturati in attività riconducibili alla sicurezza informatica.

3.1.9 Junior Security Consultant

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale che fornisce supporto consulenziale e tecnico-operativo nell'ambito dei servizi di cybersecurity previsti dal Capitolato, operando sotto il coordinamento delle figure senior e

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
Missione e ambito di intervento	contribuendo all'esecuzione delle attività di analisi, verifica e supporto alla sicurezza dei sistemi informativi dell'Amministrazione.
	Opera nell'ambito dei servizi previsti dal Capitolato supportando le attività di cybersecurity attraverso l'esecuzione di analisi tecniche, verifiche operative e attività di supporto , contribuendo all'implementazione delle misure di sicurezza e alla raccolta delle evidenze necessarie, in coerenza con le indicazioni fornite dalle figure di governo e di consulenza senior. La figura concorre all'erogazione dei servizi con un ruolo prevalentemente esecutivo e di supporto , maturando esperienza operativa e metodologica nei principali ambiti della sicurezza delle informazioni.
	Il Junior Security Consultant deve possedere competenze di base e in progressivo consolidamento in ambito cybersecurity e, in particolare, è in grado di: – supportare le attività di Continuous Vulnerability Management, collaborando alla raccolta e organizzazione delle informazioni, all'esecuzione delle verifiche previste e alla predisposizione delle evidenze e della documentazione di supporto; – supportare le attività di gestione delle identità e degli accessi, collaborando alle attività di verifica degli accessi, revisione delle autorizzazioni e controllo dell'applicazione dei modelli operativi definiti; – collaborare alla predisposizione e all'aggiornamento della documentazione tecnica, report di attività e contributi a supporto delle analisi svolte dalle figure senior; – applicare i processi e le procedure operative IT e di sicurezza definiti dall'Amministrazione e dal Fornitore, operando nel rispetto degli standard e delle linee guida adottate; – operare in coordinamento con le figure di consulenza senior e con i team operativi, contribuendo al corretto svolgimento delle attività assegnate e al rispetto delle tempistiche previste.
Competenze ed esperienze richieste	
Certificazioni	Non richieste
Titolo di studio	Laurea triennale in discipline tecnico-scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 3 (tre) anni in ambito ICT, di cui almeno 2 (due) maturati in attività riconducibili alla cybersecurity o alla sicurezza delle informazioni.

3.1.10 Legal, Policy and Compliance Officer

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale specializzata nel supporto giuridico-normativo e di compliance in ambito cybersecurity, sicurezza delle informazioni e protezione dei dati, che affianca l'Amministrazione nell'interpretazione, applicazione e verifica del rispetto del quadro normativo, regolatorio e di policy applicabile.
Missione e ambito di intervento	Opera nell'ambito dei servizi previsti dal Capitolato fornendo supporto consulenziale e operativo-metodologico alle strutture dell'Amministrazione e alle figure di governo della sicurezza, con particolare riferimento: – all'allineamento dei servizi di cybersecurity ai requisiti normativi e regolatori applicabili; – alla formalizzazione e verifica di policy, procedure e modelli organizzativi di sicurezza; – al presidio degli adempimenti di compliance connessi alle attività tecniche e operative svolte nell'ambito dei Contratti Esecutivi.
Competenze ed esperienze richieste	La figura deve possedere comprovata esperienza in contesti complessi e, in particolare, è in grado di: – supportare l'Amministrazione nella lettura e applicazione del quadro normativo nazionale ed europeo in materia di cybersecurity e protezione dei dati (a titolo esemplificativo: Legge n. 90 del 2024, recante «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici»; GDPR, NIS2, DORA, Linee guida ACN, Linee guida AgID);

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	– fornire supporto alla verifica di conformità normativa dei servizi di cybersecurity erogati (es. gestione delle vulnerabilità, incident management, gestione accessi e identità, supporto specialistico); – collaborare alla definizione, aggiornamento e verifica di policy e procedure in ambito sicurezza delle informazioni, protezione dei dati e gestione degli accessi, assicurandone la coerenza con i requisiti legali e organizzativi; – supportare le attività di valutazione dei rischi di compliance e di impatto normativo, incluse le valutazioni di impatto sulla protezione dei dati e le analisi di conformità a framework e standard di sicurezza; – supportare l'Amministrazione nella predisposizione della documentazione a supporto di audit, verifiche di conformità, controlli interni o richieste delle autorità competenti; – contribuire alla valutazione degli impatti e dei rischi di sicurezza connessi ai contratti di servizio, ai fornitori e alle terze parti coinvolte; – collaborare con le altre figure professionali coinvolte nei servizi di cybersecurity (es. Security Principal, Information Security Manager, Senior Security Consultant), garantendo l'allineamento tra requisiti normativi, processi di sicurezza e attività operative; – supportare la produzione di report, note di sintesi e contributi documentali a supporto dei processi decisionali dell'Amministrazione.
Certificazioni	Possesso di almeno una delle seguenti certificazioni: – Certified Information Privacy Professional/Europe (CIPP/E); – Certified Information Systems Security Professional (CISSP); per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al profilo professionale, nell'ambito di ciascun Contratto Esecutivo. Le certificazioni devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea magistrale in discipline giuridiche e/o tecnico-scientifiche, oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.

VOCE	DESCRIZIONE
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 5 (cinque) anni, maturata successivamente al conseguimento del titolo di laurea, di cui almeno 3 (tre) anni in attività riconducibili a compliance normativa, protezione dei dati, cybersecurity governance o ambiti affini.

3.1.11 Threat intelligence specialist

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale specializzata nella raccolta, analisi e contestualizzazione delle informazioni sulle minacce informatiche , finalizzate a supportare l'Amministrazione nella comprensione del panorama delle minacce, delle tecniche di attacco e dei potenziali impatti sulla postura di sicurezza.
Missione e ambito di intervento	Opera esclusivamente nell'ambito dei servizi di Continuous Vulnerability Management (CVM), con particolare riferimento alle attività di analisi e integrazione dei risultati provenienti da fonti eterogenee (inclusa la threat intelligence) e alla valutazione periodica della postura di sicurezza.
Competenze ed esperienze richieste	Il Threat Intelligence Specialist deve possedere comprovata esperienza in contesti ICT complessi e, in particolare: – raccolta e analisi di informazioni sulle minacce informatiche provenienti da fonti interne ed esterne; – analisi di indicatori di compromissione (IOC), tattiche, tecniche e procedure (TTP) degli attori di minaccia; – capacità di correlare le informazioni di threat intelligence con eventi di sicurezza, vulnerabilità e contesto operativo dell'Amministrazione; – conoscenza dei principali framework di threat intelligence e threat modeling (es. modelli di analisi delle minacce e delle campagne di attacco); – supporto alle attività di valutazione del rischio e di definizione delle priorità di sicurezza; – collaborazione con i team di security per il miglioramento delle capacità di detection e prevenzione; – produzione di report di threat intelligence, analisi contestuali e note di sintesi a supporto dei processi decisionali; – aggiornamento continuo sul panorama delle minacce, sulle vulnerabilità emergenti e sulle evoluzioni degli attori di minaccia; – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo.
Certificazioni	Possesso di almeno una delle seguenti certificazioni in ambito cybersecurity e threat intelligence:

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	– Certified Threat Intelligence Analyst (CTIA); – CompTIA CySA+ – CompTIA Cybersecurity Analyst; – GIAC Cyber Threat Intelligence (GCTI). per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo. Le certificazioni devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea triennale o magistrale in discipline tecnico-scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 5 (cinque) anni in ambito ICT, di cui almeno 3 (tre) maturati in attività riconducibili alla cybersecurity, alla threat intelligence o all'analisi delle minacce informatiche.

3.1.12 Incident responder

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale specializzata nella gestione operativa degli incidenti di sicurezza informatica , responsabile delle attività di analisi tecnica avanzata, contenimento e mitigazione degli eventi di sicurezza che impattano i sistemi informativi dell'Amministrazione.
Missione e ambito di intervento	L'Incident Responder opera nell'ambito dei servizi previsti dal Capitolato, in particolare nei servizi di incident management e security operation, supportando l'Amministrazione nella gestione degli incidenti di sicurezza lungo l'intero ciclo di vita dell'incidente, dalla rilevazione alla chiusura. La figura interviene a supporto delle attività di risposta agli incidenti, collaborando con le altre figure del team e con i referenti dell'Amministrazione, assumendo responsabilità operative nell'esecuzione delle attività di risposta agli incidenti.
Competenze ed esperienze richieste	L'Incident Responder deve possedere comprovata esperienza nella gestione degli incidenti di sicurezza in contesti ICT complessi e, in particolare:

VOCE	DESCRIZIONE
	– gestione dei processi di incident handling ed escalation per incidenti di sicurezza informatica; – analisi tecnica approfondita degli eventi di sicurezza e supporto al contenimento e alla mitigazione delle minacce; – conoscenza dei processi di analisi forense, acquisizione degli elementi probatori e conservazione degli stessi; – analisi degli attacchi e delle tecniche utilizzate, incluse attività di malware analysis e reverse engineering a livello tecnico; – conoscenza approfondita dei protocolli di rete e delle tipologie di traffico, con capacità di analisi forense del traffico di rete e identificazione di anomalie; – utilizzo avanzato di sistemi di monitoraggio, correlazione e risposta agli incidenti; – supporto alle attività di ripristino dei sistemi e verifica dell'efficacia delle azioni correttive adottate; – produzione di report tecnici di incidente e contributo alle attività di post-incident review e lesson learned; – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo per la gestione degli incidenti di sicurezza.
Certificazioni	Non richieste
Titolo di studio	Laurea triennale o magistrale in discipline tecnico scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 6 (sei) anni in ambito ICT, di cui almeno 3 (tre) maturati in attività direttamente riconducibili alla gestione degli incidenti di sicurezza, alla security operation o alla digital forensics.

3.1.13 Information Security Manager

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale responsabile del coordinamento, della gestione e del controllo delle attività di sicurezza delle informazioni , con il compito di supportare l'Amministrazione nella definizione, attuazione e monitoraggio delle misure di sicurezza, in coerenza con le politiche, gli standard e i requisiti normativi applicabili.
Missione e ambito di intervento	Opera nell'ambito dei servizi previsti dal Capitolato con riferimento alla governance della sicurezza delle informazioni , contribuendo alla pianificazione, al coordinamento e al controllo delle attività di cybersecurity, alla gestione dei rischi, alla supervisione dei processi e al raccordo tra le diverse funzioni coinvolte nella sicurezza ICT dell'Amministrazione.
Competenze ed esperienze richieste	L'Information Security Manager deve possedere comprovata esperienza in contesti ICT complessi e, in particolare: – definizione e aggiornamento delle politiche di sicurezza delle informazioni e delle procedure operative correlate; – coordinamento delle attività di sicurezza ICT e supervisione delle figure tecniche coinvolte nell'erogazione dei servizi; – supporto ai processi di gestione del rischio in ambito sicurezza delle informazioni; – pianificazione e controllo delle attività di sicurezza in coerenza con gli obiettivi dell'Amministrazione; – monitoraggio dell'attuazione delle misure di sicurezza e verifica del rispetto delle politiche e delle procedure definite; – supporto alle attività di audit, verifica e reporting in materia di sicurezza delle informazioni; – coordinamento delle attività di gestione degli eventi e degli incidenti di sicurezza, in raccordo con le figure operative competenti; – supporto all'Amministrazione nei rapporti con fornitori e terze parti per gli aspetti di sicurezza delle informazioni; – supporto all'Amministrazione e al Security Principal nella valutazione delle opzioni decisionali e nella gestione delle tematiche di sicurezza delle informazioni più complesse e sensibili, anche in relazione ai rapporti con stakeholder interni ed esterni;

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	– redazione di documentazione di sintesi, report direzionali e contributi a supporto dei processi decisionali; – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo.
Certificazioni	Possesso di almeno una delle seguenti certificazioni: – CISSP – Certified Information Systems Security Professional ((ISC)² – International Information System Security Certification Consortium); – CISM – Certified Information Security Manager (ISACA – Information Systems Audit and Control Association); – CompTIA Security+ (Computing Technology Industry Association); per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun Contratto Esecutivo. Le certificazioni devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea magistrale in discipline tecnico-scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 8 (otto) anni in ambito ICT, di cui almeno 5 (cinque) maturati in attività di sicurezza delle informazioni, cybersecurity o governance della sicurezza.

3.1.14 Senior Penetration Tester

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale specializzata nella valutazione avanzata dell'efficacia dei controlli di cybersicurezza e nell'individuazione di vulnerabilità di sicurezza su sistemi, reti, applicazioni e infrastrutture ICT, mediante attività strutturate di penetration testing ed ethical hacking.
Missione e ambito di intervento	Opera nell'ambito dei servizi previsti dal Capitolato, in particolare nei servizi di penetration testing , conducendo test di sicurezza avanzati nel rispetto delle regole di ingaggio concordate e contribuendo alla valutazione del livello di esposizione al rischio dell'Amministrazione.

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
Competenze ed esperienze richieste	Il Penetration Tester Senior deve possedere comprovata esperienza in contesti ICT complessi e, in particolare: – progettazione ed esecuzione di attività di penetration testing avanzato su infrastrutture, sistemi, reti e applicazioni; – sviluppo di script e programmi per verificare la cybersicurezza di sistemi, reti e applicazioni. – utilizzo di tecniche di ethical hacking, incluse attività controllate di ingegneria sociale; – identificazione, sfruttamento e validazione delle vulnerabilità di sicurezza; – esecuzione di analisi statica, dinamica e mobile del codice e delle configurazioni di sistema; – utilizzo avanzato di strumenti e framework di penetration testing; – analisi delle vulnerabilità senza impatto sull'operatività dei sistemi in esercizio; – supporto ai processi di hardening di sistemi e piattaforme middleware; – verifica dell'efficacia delle azioni di remediation adottate a seguito delle attività di test; – produzione di report tecnici dettagliati, comprensivi di evidenze, scenari di attacco e raccomandazioni; – capacità di coordinamento operativo di risorse junior nell'ambito delle attività di penetration testing; – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo.
Certificazioni	Possesso di almeno una tra le seguenti certificazioni in ambito penetration testing ed ethical hacking, tra: – OSCP – Offensive Security Certified Professional; – OPST – OSSTMM Professional Security Tester; – CEH – Certified Ethical Hacker;

VOCE	DESCRIZIONE
	per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo. Le certificazioni devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea magistrale in discipline tecnico-scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 10 (dieci) anni in ambito ICT, di cui almeno 5 (cinque) maturati in attività riconducibili al penetration testing o alla sicurezza offensiva.

3.1.15 Junior Penetration Tester

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale che supporta le attività di valutazione dell'efficacia dei controlli di cybersicurezza e di individuazione delle vulnerabilità di sicurezza di sistemi e infrastrutture ICT, operando sotto il coordinamento di figure senior.
Missione e ambito di intervento	Opera nell'ambito dei servizi previsti dal Capitolato, in particolare nei servizi di penetration testing, contribuendo all'esecuzione delle attività di test di sicurezza nel rispetto delle regole di ingaggio definite e delle metodologie adottate.
Competenze ed esperienze richieste	Il Penetration Tester Junior deve possedere esperienza in ambito ICT e, in particolare: – partecipazione allo sviluppo e all'utilizzo di script e strumenti di penetration testing; – supporto alle attività di ethical hacking e di ingegneria sociale controllata; – utilizzo di tool di penetration testing per l'analisi di sistemi, reti e applicazioni; – supporto alle attività di analisi tecnica e di reporting; – contributo all'identificazione delle vulnerabilità e dei controlli di sicurezza inefficaci; – partecipazione alle attività di analisi statica, dinamica e mobile del codice e delle configurazioni di sistema; – supporto ai processi di hardening di sistemi e piattaforme middleware; – documentazione delle attività di test svolte, al fine di garantirne la ripetibilità; – partecipazione alla verifica dell'efficacia delle misure di remediation adottate; – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo.
Certificazioni	Non richieste.
Titolo di studio	Diploma di scuola secondaria di secondo grado in discipline tecnico-scientifiche oppure titolo di studio superiore o cultura equivalente, secondo quanto previsto dal Capitolato.

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 3 (tre) anni in ambito ICT, di cui almeno 2 (due) maturati in attività riconducibili alla sicurezza informatica o al penetration testing.

3.1.16 AI Security Specialist

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale specializzata nel supporto tecnico-specialistico alla sicurezza delle soluzioni basate su tecnologie di Intelligenza Artificiale e Machine Learning, che opera in affiancamento all'Amministrazione nelle attività di valutazione, analisi e verifica della sicurezza delle componenti AI/ML.
Missione e ambito di intervento	Opera nell'ambito del Servizio di Supporto specialistico previsto dal Capitolato, fornendo contributi tecnici e metodologici alla sicurezza delle soluzioni AI/ML adottate o in fase di adozione dall'Amministrazione. La figura opera con un ruolo di supporto tecnico-specialistico e affiancamento operativo, contribuendo alla valutazione, verifica e rafforzamento della sicurezza delle soluzioni AI/ML, nel rispetto dei processi, delle policy e delle architetture dell'Amministrazione.
Competenze ed esperienze richieste	L'AI Security Specialist possiede esperienza in contesti ICT complessi e, in particolare, è in grado di: – supportare l'analisi della superficie di esposizione delle soluzioni AI/ML, includendo modelli, pipeline di training e inferenza, dataset, servizi applicativi e integrazioni; – contribuire alla valutazione dei rischi di sicurezza specifici delle soluzioni AI/ML, con riferimento a dati, modelli, API, pipeline e configurazioni; – supportare l'analisi delle relazioni di dipendenza e della supply chain delle componenti AI/ML, incluse dipendenze tecnologiche, componenti di terze parti, modelli pre addestrati e dataset; – fornire contributi tecnici alle attività di testing e verifica della sicurezza delle soluzioni AI/ML, inclusi aspetti di robustezza, esposizione delle API, uso improprio e scenari di abuso; – collaborare alla definizione e verifica di misure tecniche e procedurali di mitigazione, coerenti con le architetture e i controlli di sicurezza dell'Amministrazione; – supportare la verifica dell'auditabilità tecnica delle soluzioni AI/ML, inclusa la capacità di produrre evidenze e report di sicurezza in formati aperti, verificabili e privi di dipendenze da strumenti proprietari non documentati;

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	– contribuire alla produzione di documentazione tecnica e note di supporto relative alla sicurezza delle soluzioni AI/ML; – operare in coordinamento con le altre figure professionali coinvolte nei servizi di cybersecurity previsti dal Capitolato, assicurando coerenza operativa e integrazione delle attività; – contribuire alle attività di formazione tecnica e awareness in ambito AI Security, mediante supporto specialistico, sessioni di affiancamento e trasferimento di competenze verso il personale dell'Amministrazione, in coerenza con il perimetro dei servizi previsti dal Capitolato.
Certificazioni	Non richieste
Titolo di studio	Laurea magistrale in discipline tecnico-scientifiche oppure cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 6 (sei) anni in ambito ICT, di cui almeno 2 (due) anni maturati in attività riconducibili alla sicurezza delle applicazioni, dei sistemi o di soluzioni data-driven e AI-based (quali, a titolo esemplificativo, sistemi di analisi avanzata dei dati, pipeline di trattamento dati a supporto di modelli AI/ML o servizi digitali basati su logiche data-centriche).

3.1.17 Security Engineer

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale specializzata nella implementazione, configurazione e gestione tecnica delle soluzioni di sicurezza informatica , a supporto dei servizi di cybersecurity previsti dal Capitolato.
Missione e ambito di intervento	Il Security Engineer opera nell'ambito dei servizi previsti dal Capitolato, in particolare nei servizi di security operation, sicurezza dei sistemi e delle applicazioni, gestione delle vulnerabilità e supporto specialistico. La figura contribuisce all'implementazione e al corretto funzionamento delle soluzioni di sicurezza, operando in coordinamento con le altre figure del team e con i referenti dell'Amministrazione.
Competenze ed esperienze richieste	Il Security Engineer deve possedere comprovata esperienza tecnica in contesti ICT complessi e, in particolare: – implementazione, configurazione e gestione di soluzioni di sicurezza informatica su infrastrutture, sistemi e applicazioni; – conoscenza delle principali tecnologie di sicurezza (es. sistemi di protezione perimetrale, soluzioni endpoint, sistemi di monitoraggio e detection, Identity & Access Management); – configurazione, aggiornamento e gestione tecnica delle soluzioni di sicurezza, nell'ambito delle attività operative di cybersecurity; – supporto alle attività di vulnerability management, hardening e verifica delle configurazioni di sicurezza, incluse le attività tecniche di supporto al patching di sicurezza; – capacità di analisi tecnica delle configurazioni e individuazione di misconfigurazioni o criticità di sicurezza; – collaborazione, anche a titolo esemplificativo, con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity (quali Security Architect, Security Analyst e Incident Responder), al fine di garantire il corretto funzionamento delle soluzioni di sicurezza;

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	– produzione di documentazione tecnica e contributo alla reportistica di servizio.
Certificazioni	Possesso di certificazioni in ambito cybersecurity e tecnologie di sicurezza, tra: – CompTIA Security+ (CompTIA Security Plus), in ambito sicurezza delle informazioni; – CompTIA CySA+ (CompTIA Cybersecurity Analyst), in ambito analisi tecnica e gestione delle minacce; – CISSP (Certified Information Systems Security Professional), in ambito architetture e controlli di sicurezza, per profili con maggiore seniority; – eventuale possesso di certificazioni vendor-specific in ambito sicurezza; per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo. Le certificazioni, se possedute, devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea triennale o magistrale in discipline tecnico scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 6 (sei) anni in ambito ICT, di cui almeno 4 (quattro) maturati in attività riconducibili all'implementazione o gestione tecnica di soluzioni di cybersecurity.

3.1.18 Network Security Engineer

VOCE	DESCRIZIONE
Descrizione sintetica	Figura professionale specializzata nella progettazione, configurazione, gestione e messa in sicurezza delle infrastrutture di rete , con particolare riferimento ai sistemi di protezione perimetrale, ai meccanismi di controllo del traffico e alle soluzioni di network security.
Missione e ambito di intervento	Opera nell'ambito dei servizi previsti dal Capitolato con riferimento alla sicurezza delle reti e delle comunicazioni , contribuendo alla realizzazione, alla configurazione e alla gestione delle architetture di rete sicure, alla protezione del perimetro e alla difesa delle infrastrutture di rete dell'Amministrazione, in coerenza con le politiche e le architetture di sicurezza definite.
Competenze ed esperienze richieste	Il Network Security Engineer deve possedere comprovata esperienza in contesti ICT complessi e, in particolare: – progettazione e gestione di architetture di rete sicure in ambienti enterprise; – configurazione e gestione di firewall, sistemi di protezione perimetrale, VPN, IDS/IPS, proxy e soluzioni di network segmentation; – implementazione di politiche di sicurezza di rete, filtraggio del traffico e controllo degli accessi; – gestione e messa in sicurezza delle comunicazioni di rete, incluse reti WAN, LAN e ambienti virtualizzati; – supporto alle attività di hardening delle infrastrutture di rete; – analisi delle configurazioni di rete e individuazione di vulnerabilità o misconfigurazioni; – integrazione delle soluzioni di network security con i sistemi di monitoraggio e logging; – supporto tecnico alle attività di gestione degli eventi di sicurezza che coinvolgono la rete; – redazione di documentazione tecnica relativa alle architetture e alle configurazioni di rete; – collaborazione con le altre figure professionali coinvolte nell'erogazione dei servizi di cybersecurity, al fine di garantire il corretto svolgimento delle attività e il coordinamento operativo.
Certificazioni	Possesso di almeno una delle seguenti certificazioni:

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

VOCE	DESCRIZIONE
	- CompTIA Network+ (Computing Technology Industry Association – Network Plus); - CompTIA Security+ (Computing Technology Industry Association – Security Plus); - CCNA – Cisco Certified Network Associate oppure CCNP Security – Cisco Certified Network Professional Security; - Fortinet NSE 4 o NSE 5 – Fortinet Network Security Expert, livello 4 o 5 (o certificazioni equivalenti nell'ambito del programma di certificazione Fortinet); - PCNSE – Palo Alto Networks Certified Network Security Engineer o certificazioni equivalenti nell'ambito del programma di certificazione Palo Alto Networks. per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo. Le certificazioni devono essere in corso di validità per tutta la durata del Contratto Esecutivo.
Titolo di studio	Laurea triennale o magistrale in discipline tecnico-scientifiche oppure titolo di studio diverso accompagnato da cultura equivalente, secondo quanto previsto dal Capitolato.
Anzianità lavorativa	Esperienza professionale complessiva non inferiore a 4 (quattro) anni in ambito ICT, di cui almeno 2 (due) maturati in attività di network security o sicurezza delle infrastrutture di rete.

3.1.19 Valutazione dei curricula

I curriculum vitae delle figure professionali da impiegare nei vari servizi dovranno essere resi disponibili alle Amministrazioni rispettando lo schema indicato al capitolo 5. Sarà facoltà dell'Amministrazione indicare un diverso template. In ogni caso, dovranno essere particolarmente dettagliate le competenze ed esperienze tecniche al fine di verificare la corrispondenza con i requisiti minimi, gli eventuali requisiti migliorativi offerti e il contesto dell'Amministrazione.

Sulla base dei CV presentati l'Amministrazione procederà alla verifica che il personale proposto sia in linea con i requisiti minimi e gli eventuali requisiti migliorativi offerti, riservandosi la possibilità di procedere ad un colloquio di approfondimento per verificare la corrispondenza delle competenze elencate nel CV (in tal caso il Fornitore dovrà rendere disponibile al colloquio la risorsa **entro 3 giorni lavorativi** dalla richiesta). Per il personale ritenuto inadeguato, qualunque sia il ruolo, l'Amministrazione Contraente procederà alla richiesta formale di sostituzione inviando apposita richiesta di sostituzione, in cui indicherà puntualmente la risorsa che ritiene inadeguata, le relative motivazioni in riferimento ai requisiti minimi e/o migliorativi di gara, la "data prevista di sostituzione" ai fini degli indicatori di qualità. La presentazione del CV (e delle eventuali certificazioni) della nuova risorsa in sostituzione dovrà quindi avvenire secondo i termini indicati dall'Amministrazione (che non potranno superare i 5 giorni lavorativi). La richiesta di sostituzione potrà avvenire anche successivamente all'avvio del servizio, laddove l'Amministrazione riscontri che il personale impiegato non sia adeguato ad effettuare le attività richieste.

Il Fornitore, in caso necessiti di sostituire il personale allocato presso l'Amministrazione, dovrà darne opportuna comunicazione all'Amministrazione stessa entro 10 giorni lavorativi dalla sostituzione della stessa, indicando al contempo la nuova risorsa subentrante e inviando il relativo CV (e le eventuali certificazioni). La nuova risorsa dovrà possedere tutte le caratteristiche di quella in sostituzione. L'Amministrazione valuterà il nuovo CV, anche mediante colloquio, ai fini dell'autorizzazione alla sostituzione.

Ciascuna risorsa impiegata dovrà fornire, nel corso dell'esecuzione dei servizi, la propria esperienza sullo specifico ambito di competenza, a supporto dell'erogazione dei servizi medesimi, interagendo con l'Amministrazione e/o con i soggetti terzi da essa delegati e con i vari gruppi di lavoro coinvolti.

Oltre a tali attività, le risorse impiegate avranno il compito di divulgare all'interno dell'Amministrazione la conoscenza maturata sui progetti seguiti e sui servizi erogati, attraverso riunioni, presentazioni e documenti di best practices in modo da rendere il personale dell'Amministrazione consapevole di quanto realizzato in ambito cybersecurity e del valore aggiunto apportato all'Amministrazione medesima.

I Fornitori potranno offrire l'impiego, in fase di esecuzione, di personale in possesso di certificazioni in ambito *security* secondo quanto previsto nel Capitolato d'Oneri.

4 INDICATORI DI QUALITÀ

Il presente capitolo definisce il livello di qualità minimo atteso dei servizi dei singoli Contratti Esecutivi, attraverso la definizione degli obiettivi di qualità, la misura del loro raggiungimento e il dettaglio delle azioni contrattuali da applicare in caso di mancato rispetto dei valori soglia (indicatori di qualità).

Il Fornitore potrà integrare i presenti indicatori nell'ambito dell'Offerta Tecnica presentata ai fini dell'aggiudicazione dell'Accordo Quadro, secondo i criteri indicati nel Capitolato d'Oneri.

Il mancato rispetto dei valori di soglia migliorativi sarà sanzionato con la penale "Mancato rispetto degli impegni assunti in offerta tecnica".

Per gli indicatori di qualità di cui al presente capitolo, le conseguenti azioni contrattuali potranno essere esercitate dalle singole Amministrazioni od essere esercitate da Consip S.p.A., ove previsto, su richiesta delle Amministrazioni.

Su richiesta dell'Amministrazione, il Fornitore dovrà fornire i dati elementari utilizzati per il calcolo degli indicatori di cui al presente paragrafo.

Tali dati dovranno essere forniti in un formato elaborabile con i prodotti di office automation in uso presso l'Amministrazione. Inoltre, il Fornitore dovrà mettere a disposizione delle Amministrazioni, senza oneri aggiuntivi, uno strumento per la fruizione dei suddetti contenuti.

Relativamente alle penali per ritardo, si precisa inoltre che deve considerarsi ritardo anche il caso in cui il Fornitore esegua le prestazioni relative allo specifico indicatore in modo anche solo parzialmente difforme dalle disposizioni di cui al presente documento, all'Offerta tecnica e comunque alle indicazioni contenute nel Piano di Lavoro Generale. In tal caso, le Amministrazioni applicheranno al Fornitore le penali di cui allo specifico indicatore sino alla data in cui la fornitura inizierà ad essere eseguita in modo effettivamente conforme, fatto salvo il risarcimento del maggior danno.

4.1 IQ01 – Rispetto di una scadenza contrattuale

L'indicatore misura il rispetto di scadenze temporali derivanti dalla documentazione contrattuale (dell'Accordo Quadro e del Contratto Esecutivo), dal Piano di Lavoro Generale e comunque concordate con l'Amministrazione. La penale prevista nel presente paragrafo riveste carattere residuale rispetto ad altre penali da ritardo espressamente normate nel presente documento e in ogni caso nell'Accordo Quadro e relativi allegati, nonché nel Contratto Esecutivo, ossia verrà applicato tale indicatore se non ve ne sono altri specifici.

A titolo esemplificativo e non esaustivo si rappresentano di seguito alcuni documenti, il cui ritardo nella trasmissione può determinare l'applicazione di penali:

- Adempimenti relativi alle fasi di invio del Piano Operativo e di perfezionamento del Contratto Esecutivo di cui ai rispettivi paragrafi del Capitolato Tecnico Generale;

- Piani di qualità generale e specifico;
- Piano di lavoro Generale;
- CV delle risorse e dei responsabili tecnici con le relative certificazioni;
- Deliverable di fornitura.

ASPETTO DA VALUTARE	RISPETTO DI UNA SCADENZA CONTRATTUALE		
Unità di misura	Giorni lavorativi	Fonte dati	Comunicazioni Note Amministrazione Verballi di riunioni
Periodo di riferimento	Durata della fornitura Periodi di verifica di conformità	Frequenza di misurazione	Mensile o a scadenza se minore
Dati da rilevare	Per ciascuna scadenza vanno rilevati: – Data prevista (data_prev) – Data effettiva (data_eff) L'indicatore viene calcolato come sommatoria degli eventi rilevati nel periodo di misurazione (mensile)		
Regole di campionamento	Nessuna		
Formula	$IQ01 = \sum (data_eff - data_prev)$		
Regole di arrotondamento	Nessuna		
Valore di soglia	$IQ01 = 1$		
Azioni contrattuali	Il mancato rispetto del valore di soglia comporterà <u>per ogni giorno (solare o lavorativo a seconda di quanto indicato nel corrispondente paragrafo di riferimento) di ritardo rispetto al valore soglia</u> l'applicazione della penale “Mancato rispetto di una scadenza contrattuale dell’Accordo Quadro” , pari a 5.000,00 (cinquemila/00). Il mancato rispetto del valore di soglia comporterà <u>per ogni giorno (solare o lavorativo a seconda di quanto indicato nel corrispondente paragrafo di riferimento) di ritardo rispetto al valore soglia</u> l'applicazione della penale “Mancato rispetto di una		

	scadenza contrattuale del Contratto esecutivo ", pari all'0,6% (zerovirgolasei per mille), dell'importo del Contratto esecutivo.
Applicazione	Consip e Amministrazione Contraente
Eccezioni	Nessuna

4.2 IQ02 – Adeguatezza delle figure professionali proposte per la erogazione dei servizi

L'indicatore misura il numero di figure professionali impiegate nell'erogazione dei servizi (diversi da Responsabile unico delle attività contrattuali e Responsabili tecnici del Fornitore per l'erogazione dei servizi) che, nel corso della fornitura, l'Amministrazione Contraente abbia ritenuto non rispondenti al profilo professionale richiesto, richiedendone la sostituzione;

ASPETTO VALUTARE	DA	NUMERO DI RISORSE IMPIEGATE NELLA EROGAZIONE DEL SERVIZIO RITENUTE DALL'AMMINISTRAZIONE NON RISPONDENTI AI REQUISITI		
Unità di misura		Risorsa inadeguata	Fonte dati	E-mail Lettere Verbali
Periodo di riferimento		Durata della fornitura	Frequenza di misurazione	Mensile
Dati da rilevare		N_{ris_inad} = Numero di risorse sostituite su richiesta dell'Amministrazione perché non rispondenti ai requisiti		
Regole campionamento	di	Nessuna		
Formula		$IQ02 = N_{ris_inad}$		
Regole arrotondamento	di	Nessuna		
Valore di soglia		$IQ02 = 1$		
Azioni contrattuali		Il mancato rispetto del valore di soglia comporterà <u>per ogni risorsa eccedente il valore di soglia nel periodo di riferimento</u> l'applicazione della penale "Risorse Impiegate nell'erogazione del servizio non rispondenti ai requisiti" , pari all'0,6% (zerovirgolasei per mille), dell'importo del Contratto esecutivo.		
Applicazione		Amministrazione Contraente		
Eccezioni		Nessuna		

4.3 IQ03 – Adeguatezza del personale impiegato nei ruoli contrattuali

L'indicatore misura il numero di risorse nei ruoli di Responsabile unico delle attività contrattuali (RUAC dell'Accordo Quadro) e di Responsabili tecnici del Fornitore che, nel corso della fornitura, Consip o l'Amministrazione Contraente abbia ritenuto non rispondente al profilo professionale richiesto nel Capitolato Tecnico Generale, richiedendone la sostituzione.

ASPETTO DA VALUTARE	NUMERO DI RISORSE RITENUTE INADEGUATE		
Unità di misura	Risorsa inadeguata	Fonte dati	E-mail Lettere Verbali
Periodo di riferimento	Durata della fornitura	Frequenza di misurazione	Mensile
Dati da rilevare	N_{ris_inad} = Numero di risorse sostituite per inadeguatezza su richiesta di Consip o dell'Amministrazione		
Regole di campionamento	Nessuna		
Formula	$IQ103 = N_{ris_inad}$		
Regole di arrotondamento	Nessuna		
Valore di soglia	$IQ03 = 0$		
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per la sostituzione del RUAC dell'Accordo Quadro rispetto al valore soglia</u> l'applicazione della penale "Adeguatezza del personale impiegato nei ruoli contrattuali" pari a € 5.000,00 (cinquemila/00). Il mancato rispetto del valore soglia comporterà <u>per ogni risorsa di Responsabile tecnico del Fornitore sostituito rispetto al valore soglia</u> l'applicazione della penale "Adeguatezza del personale impiegato nei ruoli contrattuali" pari all'0,6% (zerovirgolasei per mille) dell'importo del Contratto esecutivo.		
Applicazione	Consip e Amministrazione Contraente		
Eccezioni	Nessuna		

4.4 IQ04 – Adeguatezza dei tempi di sostituzione delle figure professionali proposte per la erogazione dei servizi

L'indicatore misura i giorni di ritardo nella sostituzione di figure professionali (diversi da Responsabile unico delle attività contrattuali e Responsabili tecnici del Fornitore per l'erogazione dei servizi) che eccedano quelli previsti nel Capitolato tecnico speciale.

ASPETTO VALUTARE	DA	NUMERO DI GIORNI DI RITARDO NELLA SOSTITUZIONE DI RISORSE IMPIEGATE NELLA EROGAZIONE DEL SERVIZIO RITENUTE DALL'AMMINISTRAZIONE NON RISPONDENTI AI REQUISITI		
Unità di misura	Risorsa inadeguata	Fonte dati	E-mail Lettere Verbalì	
Periodo di riferimento	Durata della fornitura	Frequenza di misurazione	Mensile	
Dati da rilevare	Per ciascuna risorsa vanno rilevati: – Data prevista sostituzione (data_prev) – Data effettiva sostituzione (data_eff) L'indicatore viene calcolato come sommatoria degli eventi rilevati nel periodo di misurazione (mensile)			
Regole campionamento	di	Nessuna		
Formula	IQ04 = Σ (data_eff – data_prev)			
Regole arrotondamento	di	Nessuna		
Valore di soglia	IQ04 = 5			
Azioni contrattuali	Il mancato rispetto del valore di soglia comporterà <u>per ogni giorno (solare o lavorativo a seconda di quanto indicato nel corrispondente paragrafo di riferimento) eccedente il valore di soglia nel periodo di riferimento</u> l'applicazione della penale “Adeguatezza dei tempi di sostituzione delle figure professionali proposte per la erogazione dei servizi” , pari all'0,6‰ (zerovirgolasei per mille), dell'importo del Contratto esecutivo.			
Applicazione	Amministrazione Contraente			
Eccezioni	Nessuna			

4.5 IQ05 - Turnover del personale impiegato nella fornitura

L'indicatore misura il numero di sostituzioni delle risorse impiegate (inclusi il RUAC e Responsabili tecnici del Fornitore dell'erogazione del servizio), su iniziativa del Fornitore e non autorizzate dall'Amministrazione Contraente.

ASPETTO VALUTARE	DA	NUMERO DI RISORSE SOSTITUITE SU INIZIATIVA DEL FORNITORE		
Unità di misura		Risorse	Fonte dati	E-mail lettere verbali
Periodo riferimento	di	Durata della fornitura	Frequenza misurazione	di Mensile
Dati da rilevare		Numero risorse sostituite su iniziativa del Fornitore (<i>Nrisorse_sostituite</i>)		
Regole campionamento	di	Nessuna		
Formula		<i>IQ05 = Nrisorse_sostituite</i>		
Regole arrotondamento	di	Nessuna		
Valore di soglia		<i>IQ05 = 1</i>		
Azioni contrattuali		Il mancato rispetto del valore soglia comporterà <u>per ogni risorsa aggiuntiva rispetto al valore soglia</u> l'applicazione della penale “Turnover del personale impiegato nella fornitura” pari a € 1.000,00 (mille/00).		
Applicazione		Consip e Amministrazione Contraente		
Eccezioni		– Eventuali sostituzioni finalizzate ad un migliore funzionamento dei servizi/attività, purché preventivamente approvate dai referenti dell'Amministrazione, non contribuiscono al raggiungimento del valore soglia. – Eventuali sostituzioni operate a fronte di dimissioni/licenziamento di risorse impegnate nell'erogazione dei servizi non contribuiscono al raggiungimento del valore soglia <u>purché sia rispettata almeno una delle seguenti condizioni</u>: a) ciascuna sostituzione sia effettuata nel rispetto dei termini del preavviso previsti dal contratto di lavoro applicato;		

	b) ciascuna sostituzione deve essere preventivamente approvata dall'Amministrazione; c) ciascuna dimissione sia opportunamente documentata.
--	---

4.6 IQ06 – Impegni assunti in offerta tecnica

L'indicatore di qualità verifica il numero di impegni assunti dal Fornitore in offerta tecnica, afferenti a obbligazioni contrattuali non adempiute nei tempi e/o nei modi rappresentati nel Contratto esecutivo e relativi allegati e/o tracciati sul Piani di lavoro Generale, qualora non presidiate da specifici indicatori.

ASPETTO VALUTARE	DA	NUMERO DI IMPEGNI ASSUNTI DAL FORNITORE IN OFFERTA TECNICA NON ADEMPIUTI		
Unità di misura		Impegno	Fonte dati	Comunicazioni Note Amministrazione
Periodo riferimento	di	Durata della fornitura	Frequenza misurazione	di Mensile o a scadenza se minore
Dati da rilevare		N_IMP = Numero impegni assunti dal Fornitore in offerta tecnica		
Regole campionamento	di	Nessuna		
Formula		$IQ06 = N_IMP$		
Regole arrotondamento	di	Nessuna		
Valore di soglia		$IQ06 = 0$		
Azioni contrattuali		Il mancato rispetto del valore di soglia comporterà <u>per ogni scostamento rispetto al valore soglia</u> l'applicazione della penale “Impegni assunti in offerta tecnica” , pari all'0,6‰ (zerovirgolasei per mille), dell'importo del Contratto esecutivo.		
Applicazione		Amministrazione Contraente		
Eccezioni		Nessuna		

4.7 IQ07 – Tempestività di risposta per il servizio di Service Desk

L'indicatore di qualità è definito come la percentuale, consolidata su base mensile, di chiamate risposte entro i 120 secondi nell'ambito della finestra di erogazione del servizio con operatore, misurati tra l'inizio della chiamata al servizio di Service Desk (o dalla eventuale selezione sul risponditore automatico dell'opzione per parlare con un operatore) e la risposta dell'operatore per Contratto Esecutivo (cnf paragrafo xx del Capitolato Tecnico Generale).

ASPETTO DA VALUTARE		TEMPESTIVITÀ DI RISPOSTA PER IL SERVIZIO DI SERVICE DESK	
Unità di misura	Percentuale	Fonte dati	Comunicazioni Contratto Esecutivo Piano di Lavoro Strumenti di Tracciatura
Periodo di riferimento	di Durata della fornitura Periodi di verifiche di conformità	Frequenza di misurazione	di Mensile
Dati da rilevare	– Data e Ora (hh/mm/ss/dd) di avvio dell'interazione (<i>Data_avvio</i>) – Data e Ora (hh/mm/ss/dd) della effettiva risposta (<i>Data_risp</i>) – Numero totale interazioni pervenute nel periodo di riferimento (<i>Num_tot</i>)		
Regole campionamento	di Nessuna		
Formula	$IQ07 = Num_interazioni (T_risp \leq T_ottimale) / Num_tot$ Dove: $T_risp = Data_risp - Data_avvio$ $T_ottimale = 120 \text{ secondi}$		
Regole arrotondamento	di Il risultato della misura va arrotondato al punto percentuale: - per difetto se la parte decimale è <= 0,5 - per eccesso se la parte decimale è > 0,5		
Valore di soglia	$IQ07 = 95\%$		
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale in diminuzione rispetto al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Tempestività di risposta” pari a € 300,00 (trecento/00).		
Applicazione	Amministrazione Contraente		
Eccezioni	Nessuna		

4.8 IQ08 – Qualità complessiva dell'Asset Inventory

L'indicatore di qualità misura il livello complessivo di affidabilità dell'Asset Inventory prodotto/aggiornato dal Fornitore, valutando separatamente e congiuntamente i seguenti aspetti:

- la **copertura** degli asset identificati;
- l'**accuratezza** dei dati normalizzati;
- l'**eliminazione di incoerenze e duplicazioni**.

L'Indicatore di Qualità si considera **conforme esclusivamente qualora tutti i sotto-indicatori risultino conformi alle rispettive soglie**.

ASPETTO DA VALUTARE	QUALITÀ ATTIVITÀ DI PREDISPOSIZIONE/AGGIORNAMENTO ASSET INVENTORY:		
	- A: COPERTURA DEGLI ASSET IDENTIFICATI - B: ACCURATEZZA DEI DATI NORMALIZZATI - C: ELIMINAZIONE DI INCOERENZE E DUPLICAZIONI		
Unità di misura	Percentuale	Fonte dati	CMDB, inventari PA, strumenti di discovery, repository e fonti dati forniti dall'Amministrazione
Periodo di riferimento	Durata del servizio Consegna dei deliverable Periodi di verifiche di conformità	Frequenza di misurazione	Alla consegna e aggiornamento dei deliverable: • Asset Inventory consegnato/aggiornato • Report di assessment • Dashboard
Dati da rilevare	IQ08_A: N° asset identificati (N_identificati); N° asset attesi (N_attesi) IQ08_B: N° asset con dati corretti (N_corretti); N° asset verificati (N_verificati) IQ08_C: N° incoerenze/duplicazioni risolte (N_risolte); N° incoerenze/duplicazioni rilevate (N_rilevate)		
Regole di campionamento	Gli Indicatori di Qualità relativi al servizio di Asset Inventory sono calcolati sull'intero perimetro del deliverable consegnato e non prevedono l'applicazione di criteri di campionamento.		
Formula	$IQ08_A: (N_identificati / N_attesi) \times 100$ $IQ08_B: (N_corretti / N_verificati) \times 100$ $IQ08_C: (N_risolte / N_rilevate) \times 100$		

Regole di arrotondamento	Il risultato della misura va arrotondato al punto percentuale: – per difetto se la parte decimale è $\leq 0,5$ – per eccesso se la parte decimale è $> 0,5$
Valore di soglia	$IQ08_A \geq 95\%$ $IQ08_B \geq 95\%$ $IQ08_C \geq 95\%$
Azioni contrattuali	L'Indicatore di Qualità è considerato non conforme qualora anche uno solo dei sotto-indicatori A, B o C non risulti conforme al valore di soglia previsto. Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale in diminuzione rispetto al numero dei campioni di misura del parametro</u> nel periodo di riferimento, l'applicazione della penale “Insufficiente Qualità dati Asset Inventory” pari allo 0,6‰ (zerovirgolasei per mille), dell'importo del Contratto esecutivo.
Applicazione	Amministrazione Contraente
Eccezioni	Scostamenti imputabili a indisponibilità, incompletezza o incoerenza delle fonti informative messe a disposizione dall'Amministrazione

4.9 IQ09 – Tempestività di presa in carico del supporto di Incident ed Event Management

L'indicatore misura la tempestività con cui il Fornitore avvia le attività di supporto tecnico a seguito della segnalazione di un evento o incidente di sicurezza da parte dell'Amministrazione, in funzione della severità assegnata.

ASPETTO DA VALUTARE	TEMPESTIVITÀ DI PRESA IN CARICO DEL SUPPORTO TECNICO		
Unità di misura	Minuti/ore	Fonte dati	– Ticketing Amministrazione – Registro eventi – Verbali
Periodo di riferimento	di Durata della fornitura Periodi di verifiche di conformità	Frequenza di misurazione	di Mensile o per evento
Dati da rilevare	– Data/Ora segnalazione dell'evento/incidente – Data/Ora avvio attività di supporto del Fornitore		
Regole di campionamento	Nessuna		
Formula	IQ9 = Data_avvio_supporto – Data_segnalazione		
Regole di arrotondamento	Nessuna		
Valore di soglia	– IQ09_High_Medium: ≤ 30 minuti – IQ09_Low: ≤ 4 ore – IQ09_NONE: ≤ 1 giorno lavorativo I valori soglia potranno essere adattati dalle Amministrazioni in base alle proprie esigenze tecnico/organizzative		
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni superamento del valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Tempestività di presa in carico del supporto” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.		
Applicazione	Amministrazione Contraente		
Eccezioni	Nessuna		

4.10 IQ10 – Qualità del triage e della classificazione degli eventi

L'indicatore misura il livello di accuratezza, coerenza e qualità delle attività di triage e classificazione degli eventi di sicurezza svolte dal Fornitore, in conformità ai criteri, alle procedure e alla tassonomia adottate dall'Amministrazione.

L'indicatore tiene conto, in particolare, della corretta identificazione degli eventi non rilevanti e dei falsi positivi, della congruità delle motivazioni di classificazione e della coerenza delle decisioni assunte nel tempo.

ASPETTO VALUTARE	DA	ACCURATEZZA DEL TRIAGE E DELLA CLASSIFICAZIONE DEGLI EVENTI		
Unità di misura		Percentuale	Fonte dati	– Ticketing Amministrazione – Registro eventi – Report tecnici – Strumenti (es SIEM)
Periodo riferimento	di	Durata della fornitura Periodi di verifiche di conformità	Frequenza misurazione	di Mensile o per evento
Dati da rilevare		– Numero di eventi/alert correttamente classificati (N_corr), comprensivi di: - o eventi di sicurezza confermati; - o eventi classificati correttamente come falsi positivi; - o anomalie non rilevanti coerentemente chiuse secondo le procedure. – Numero totale di eventi/alert analizzati (N_tot).		
Regole campionamento	di	Nessuna		
Formula		$IQ10 = (N_corr / N_tot) \times 100$		
Regole arrotondamento	di	Nessuna		
Valore di soglia		– $IQ10 \geq 95\%$ <i>I valori soglia potranno essere adattati dalle Amministrazioni in base alle proprie esigenze tecnico/organizzative</i>		

Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Insufficiente qualità del triage” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo. NB: La percentuale di falsi positivi rilevata non costituisce di per sé elemento di non conformità, fermo restando l'obbligo del Fornitore di garantirne la corretta identificazione, classificazione e tracciabilità.
Applicazione	Amministrazione Contraente
Eccezioni	Nessuna

4.11 IQ11 – Conformità del supporto alle procedure dell'Amministrazione

L'indicatore misura la percentuale di eventi e incidenti per i quali il Fornitore ha fornito supporto operativo nel rispetto dei processi, delle procedure e dei playbook definiti dall'Amministrazione.

ASPETTO VALUTARE	DA	RISPETTO DELLE PROCEDURE E DEI PLAYBOOK DELL'AMMINISTRAZIONE
Unità di misura	Percentuale	Fonte dati – Ticketing Amministrazione – Registro eventi – Report tecnici – Strumenti (es SIEM) – Procedure, Playbook, istruzioni, etc dell'Amministrazione
Periodo riferimento	di	Durata della fornitura Periodi di verifiche di conformità
		Frequenza misurazione di Mensile
Dati da rilevare		– Numero alert classificati correttamente (N_corr) – Numero totale alert analizzati (N_tot)
Regole campionamento	di	Nessuna
Formula		$IQ11 = (N_corr / N_tot) \times 100$
Regole arrotondamento	di	Nessuna
Valore di soglia		– $IQ11 \geq 95\%$ <i>I valori soglia potranno essere adattati dalle Amministrazioni in base alle proprie esigenze tecnico/organizzative</i>
Azioni contrattuali		Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Insufficiente qualità del triage” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.
Applicazione		Amministrazione Contraente
Eccezioni		Nessuna

4.12 IQ12 – Efficacia del supporto specialistico senza ulteriore escalation

L'indicatore misura la percentuale di incidenti per i quali il supporto specialistico fornito dal Fornitore ha consentito di completare le attività di analisi e supporto senza la necessità di ulteriori livelli di escalation, secondo le decisioni dell'Amministrazione.

ASPETTO DA VALUTARE	GESTIONE DEGLI INCIDENTI SENZA NECESSITÀ DI ULTERIORI ESCALATION		
Unità di misura	Percentuale	Fonte dati	– Ticketing Amministrazione – Registro eventi – Report – Strumenti (es SIEM)
Periodo di riferimento	di Durata della fornitura Periodi di verifiche di conformità	Frequenza di misurazione	di Mensile o per evento
Dati da rilevare	– Incidenti gestiti senza escalation ulteriore (N_noEsc) – Incidenti totali (N_tot)		
Regole di campionamento	Nessuna		
Formula	$IQ12 = (N_noEsc / N_tot) \times 100$		
Regole di arrotondamento	Nessuna		
Valore di soglia	– $IQ12 \geq 85\%$ <i>I valori soglia potranno essere adattati dalle Amministrazioni in base alle proprie esigenze tecnico/organizzative</i>		
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Non efficacia del supporto” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.		
Applicazione	Amministrazione Contraente		
Eccezioni	Nessuna		

4.13 IQ13 – Completezza delle evidenze tecniche per decisioni e notifiche

L'indicatore misura la qualità e la completezza delle evidenze tecniche e documentali prodotte dal Fornitore a supporto delle decisioni dell'Amministrazione e delle eventuali attività di segnalazione e notifica verso le autorità competenti.

ASPETTO VALUTARE	DA	QUALITÀ E COMPLETEZZA DELLA DOCUMENTAZIONE TECNICA	
Unità di misura	Percentuale	Fonte dati	– Ticketing Amministrazione – Registro eventi – Report – Strumenti (es SIEM) – Comunicazioni Amministrazione
Periodo riferimento	di	Durata della fornitura Periodi di verifiche di conformità	di Per evento
Dati da rilevare		– Evidenze complete (N_ok) – Evidenze richieste (N_req)	
Regole campionamento	di	Nessuna	
Formula		$IQ13 = (N_ok / N_req) \times 100$	
Regole arrotondamento	di	Nessuna	
Valore di soglia		– $IQ13 \geq 95\%$ <i>I valori soglia potranno essere adattati dalle Amministrazioni in base alle proprie esigenze tecnico/organizzative</i>	
Azioni contrattuali		Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Insufficiente qualità delle evidenze tecniche” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.	
Applicazione		Amministrazione Contraente	
Eccezioni		Nessuna	

4.14 IQ14 – Copertura del perimetro assegnato

L'indicatore misura la percentuale di perimetro tecnico effettivamente trattato dal Fornitore rispetto al perimetro complessivamente assegnato dall'Amministrazione per le attività operative, sistemistiche e applicative previste nei Servizi di Sicurezza dei Sistemi e delle Applicazioni (par. 2.4) e nel Servizio di Conduzione operativa dei sistemi di sicurezza (par. 2.5).

L'indicatore verifica che tutte le componenti incluse nello scope concordato (sistemi, applicazioni, apparati di sicurezza, configurazioni operative, richieste di intervento, attività di aggiornamento, attività configurative e deliverable previsti) siano state oggetto delle attività documentate dal Fornitore.

Ai fini del presente indicatore, per "perimetro assegnato" si intende esclusivamente il perimetro di attività formalmente definito e autorizzato dall'Amministrazione nell'ambito del Piano di Lavoro Generale e/o del Contratto Esecutivo, incluse le eventuali variazioni approvate nel periodo di riferimento.

L'indicatore misura la copertura del perimetro assegnato e non la continuità temporale del servizio, che resta disciplinata dalle modalità di erogazione previste nei singoli servizi.

ASPETTO VALUTARE	DA	COPERTURA DELLE ATTIVITÀ ASSEGNATE		
Unità di misura	Percentuale	FONTE DATI	– Piano di Lavoro Generale / Contratto Esecutivo – Report tecnici dei servizi – Evidenze tecniche prodotte – Stati Avanzamento Lavori (SAL) – Comunicazioni dell'Amministrazione	
Periodo riferimento	di	Durata della fornitura Periodi di verifiche di conformità	Frequenza misurazione	di Per evento e/o secondo quanto previsto dal Piano di Lavoro Generale

Dati da rilevare	– Perimetro di attività assegnato (N_req) – Perimetro di attività effettivamente gestito dal Fornitore (N_ok) Rientrano in questa casistica: – i perimetri di analisi dei servizi di sicurezza (SAST, DAST, MAST, ecc.); – le attività configurative richieste; – la copertura dei sistemi presi in carico; – la copertura delle attività di aggiornamento / versioning.
Regole di campionamento	Nessuna
Formula	$IQ14 = (N_{ok} / N_{req}) \times 100$
Regole di arrotondamento	Nessuna
Valore di soglia	– $IQ14 \geq 95\%$ <i>I valori soglia potranno essere adattati dalle Amministrazioni in base alle proprie esigenze tecnico/organizzative</i>
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà, <u>per ogni punto percentuale inferiore</u> al valore soglia nel periodo di riferimento, l'applicazione della penale “Insufficiente copertura del perimetro assegnato” pari allo 0,5‰ (zerovirgolasei per mille) dell'importo del Contratto Esecutivo .
Applicazione	Amministrazione Contraente
Eccezioni	Sono esclusi dal calcolo i componenti del perimetro non analizzati per cause non imputabili al Fornitore, purché debitamente documentate e approvate dall'Amministrazione.

4.15 IQ15 – Completezza delle attività di sicurezza applicativa e infrastrutturale

L'indicatore misura la completezza delle attività svolte dal Fornitore per ciascun servizio di sicurezza dei sistemi e delle applicazioni rispetto allo scope e alle attività previste nel Piano di Lavoro Generale. L'indicatore verifica che, per ogni servizio attivato (SAST, DAST, MAST, Hardening, Patching, verifica dell'integrità), tutte le tipologie di attività previste (analisi, validazione, documentazione, supporto tecnico e produzione delle evidenze) siano state effettivamente eseguite.

ASPETTO VALUTARE	DA	COMPLETEZZA DELLE ATTIVITÀ DI SICUREZZA APPLICATIVA E INFRASTRUTTURALE SVOLTE DAL FORNITORE		
Unità di misura	Percentuale	Fonte dati	– Piano di Lavoro Generale / Contratto Esecutivo – Report tecnici dei servizi – Stati Avanzamento Lavori (SAL) – Evidenze tecniche e documentazione prodotta – Comunicazioni dell'Amministrazione	
Periodo riferimento	di	Durata della fornitura Periodi di verifiche di conformità	Frequenza misurazione	di Per evento e/o a conclusione delle attività previste per il servizio
Dati da rilevare		– Attività previste per il servizio attivato (N_req) – Attività effettivamente svolte e documentate (N_ok)		
Regole campionamento	di	Nessuna		
Formula		$IQ15 = (N_{ok} / N_{req}) \times 100$		
Regole arrotondamento	di	Nessuna		
Valore di soglia		– $IQ15 \geq 95\%$ <i>I valori soglia potranno essere adattati dalle Amministrazioni in base alle proprie esigenze tecnico/organizzative</i>		

Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Incompletezza delle attività di sicurezza” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.
Applicazione	Amministrazione Contraente
Eccezioni	Sono escluse dal calcolo le attività non svolte per cause non imputabili al Fornitore, purché adeguatamente motivate, tracciate e formalmente accettate dall'Amministrazione.

4.16 IQ16 – Conformità del modello di gestione delle identità (IAM)

L'indicatore misura il grado di conformità del modello di gestione delle identità e degli accessi (IAM) e delle relative procedure operative predisposte dal Fornitore rispetto ai requisiti, alle componenti minime e alla struttura formalmente definiti e approvati dall'Amministrazione nell'ambito del Piano di Lavoro Generale e/o del Contratto Esecutivo.

ASPETTO VALUTARE	DA	CONFORMITÀ DEL MODELLO E DELLE PROCEDURE IAM	
Unità di misura	Percentuale	Fonte dati	– Piano di Lavoro Generale / Contratto Esecutivo – Documento di modello operativo per la gestione degli accessi e delle identità – Policy e procedure per la gestione degli accessi e delle identità – Stati Avanzamento Lavori (SAL) – Comunicazioni dell'Amministrazione – Verbali di approvazione dell'Amministrazione
Periodo riferimento	di	Durata della fornitura Periodi di verifiche di conformità	Frequenza misurazione di Per evento e/o alla consegna dei deliverable
Dati da rilevare		– – Requisiti/componenti del modello IAM previsti (N_req) – – Requisiti/componenti del modello IAM conformi (N_ok)	
Regole campionamento	di	Nessuna	
Formula		$IQ16 = (N_{ok} / N_{req}) \times 100$	
Regole arrotondamento	di	Nessuna	

Valore di soglia	– $IQ16 \geq 95\%$ <i>I valori soglia potranno essere adattati dalle Amministrazioni in base alle proprie esigenze tecnico/organizzative</i>
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Non conformità del modello” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.
Applicazione	Amministrazione Contraente
Eccezioni	Sono esclusi dal calcolo i requisiti non valutabili per cause non imputabili al Fornitore, purché documentate e formalmente accettate dall'Amministrazione.

4.17 IQ17 – Efficacia delle attività di bonifica IAM

L'indicatore misura l'efficacia delle attività di bonifica, revisione e razionalizzazione delle identità e degli accessi svolte dal Fornitore, valutando la percentuale di anomalie effettivamente risolte rispetto a quelle formalmente accettate e autorizzate dall'Amministrazione nel periodo di riferimento.

ASPETTO VALUTARE	DA	EFFICACIA DELLE ATTIVITÀ DI BONIFICA DELLE IDENTITÀ E DEGLI ACCESSI		
Unità di misura	Percentuale	Fonte dati	– Piano di Lavoro Generale / Contratto Esecutivo – Report di attuazione operativa e controllo degli accessi – Report di bonifica di profili, account e identità – Stati Avanzamento Lavori (SAL) – Evidenze tecniche e registri di bonifica	
Periodo riferimento	di Durata della fornitura Periodi di verifiche di conformità	Frequenza misurazione	di	Periodicità e/o per evento

Dati da rilevare	– Anomalie di identità/accesso accettate nel periodo (N_acc) – Anomalie di identità/accesso risolte (N_ok)
Regole di campionamento	Nessuna
Formula	$IQ17 = (N_{ok} / N_{acc}) \times 100$
Regole di arrotondamento	Nessuna
Valore di soglia	– $IQ17 \geq 85\%$ <i>I valori soglia potranno essere adattati dalle Amministrazioni in base alle proprie esigenze tecnico/organizzative</i>
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Inefficacia delle attività di bonifica IAM” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.
Applicazione	Amministrazione Contraente
Eccezioni	Sono escluse dal calcolo le anomalie non risolvibili per cause non imputabili al Fornitore, purché tracciate e approvate dall'Amministrazione.

4.18 IQ18 – Completezza dei deliverable di Supporto specialistico

L'indicatore misura la completezza formale e contenutistica dei deliverable prodotti nell'ambito del Servizio di Supporto specialistico rispetto ai contenuti minimi, alla coerenza con l'ambito di intervento definito, alla struttura e ai requisiti previsti nel Piano di Lavoro Generale e/o nel Contratto Esecutivo.

ASPETTO VALUTARE	DA	COMPLETEZZA DEI DELIVERABLE DI SUPPORTO SPECIALISTICO	
Unità di misura	Percentuale	Fonte dati	– Piano di Lavoro Generale / Contratto Esecutivo – Deliverable SS_1 – SS_8 – Stati Avanzamento Lavori (SAL)

Periodo di riferimento	di	Durata della fornitura Periodi di verifiche di conformità	Frequenza di misurazione	di	Alla consegna dei deliverable
Dati da rilevare		- Contenuti/sezioni obbligatorie previste (N_req) - Contenuti/sezioni effettivamente presenti e conformi (N_ok)			
Regole campionamento	di	Nessuna			
Formula		$IQ18 = (N_{ok} / N_{req}) \times 100$			
Regole arrotondamento	di	Nessuna			
Valore di soglia		– $IQ18 \geq 95\%$			
Azioni contrattuali		Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Non conformità dei deliverable del supporto specialistico” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.			
Applicazione		Amministrazione Contraente			
Eccezioni		Sono esclusi dal calcolo i contenuti non producibili per cause non imputabili al Fornitore, purché documentate e accettate dall'Amministrazione.			

4.19 IQ19 – Erogazione dei moduli di formazione tecnica

L'indicatore misura il rispetto, da parte del Fornitore, delle modalità di erogazione dei moduli di formazione tecnica in conformità a quanto pianificato e approvato dall'Amministrazione, con riferimento a durata, contenuti, calendario e numero massimo di partecipanti.

ASPETTO DA VALUTARE		CONFORMITÀ DELL'EROGAZIONE DEI MODULI DI FORMAZIONE		
Unità di misura	Percentuale	Fonte dati	– Piano di Lavoro Generale – Calendari formativi – Registri presenze – Verbal di erogazione	
Periodo di riferimento	Durata della fornitura Periodi di verifiche di conformità	Frequenza di misurazione	di	Per modulo

Dati da rilevare	– Moduli formativi pianificati (N_req) – Moduli formativi erogati in conformità (N_ok)
Regole di campionamento	Nessuna
Formula	$IQ19 = (N_{ok} / N_{req}) \times 100$
Regole di arrotondamento	Nessuna
Valore di soglia	– $IQ19 \geq 95\%$
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Non conformità nell'erogazione della formazione tecnica” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.
Applicazione	Amministrazione Contraente
Eccezioni	Sono esclusi dal calcolo i moduli ripianificati su richiesta o autorizzazione dell'Amministrazione.

4.20 IQ20 – Efficacia della formazione tecnica

L'indicatore misura l'efficacia della formazione tecnica erogata dal Fornitore, valutando la percentuale di partecipanti che hanno conseguito una valutazione almeno sufficiente sulla base delle schede di valutazione previste.

ASPETTO VALUTARE	DA	EFFICACIA DELLA FORMAZIONE TECNICA	
Unità di misura	Percentuale	Fonte dati	– Piano di Lavoro Generale / Contratto Esecutivo – Schede di valutazione – Verbali di erogazione dei corsi
Periodo di riferimento	Durata della fornitura Periodi di verifiche di conformità	Frequenza di misurazione	Per modulo
Dati da rilevare	– Partecipanti valutati (N_tot) – Partecipanti con valutazione sufficiente (N_ok)		

Regole campionamento	di	Nessuna
Formula		$IQ20 = (N_{ok} / N_{tot}) \times 100$
Regole arrotondamento	di	Nessuna
Valore di soglia		– $IQ20 \geq 70\%$
Azioni contrattuali		Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Bassa efficacia della formazione tecnica” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.
Applicazione		Amministrazione Contraente
Eccezioni		Sono escluse dal calcolo le valutazioni condizionate da carenze informative o organizzative imputabili all'Amministrazione

4.21 IQ21 – Conformità dei docenti e della documentazione formativa

L'indicatore verifica la conformità dei docenti impiegati dal Fornitore per l'erogazione della formazione tecnica, nonché il rispetto delle tempistiche e dei requisiti documentali previsti per la trasmissione dei relativi curricula e delle informazioni di dettaglio.

ASPETTO VALUTARE	DA	CONFORMITÀ DEI DOCENTI E DELLA DOCUMENTAZIONE FORMATIVA	
Unità di misura	Percentuale	Fonte dati	– Piano di Lavoro Generale / Contratto Esecutivo – CV dei docenti – Comunicazioni formali – Verbali di verifica dell'Amministrazione
Periodo riferimento	di	Frequenza misurazione	di
	Durata della fornitura Periodi di verifiche di conformità		Per corso/modulo
Dati da rilevare			– Corsi/moduli erogati (N_req) – Corsi/moduli con docenti e documentazione conformi (N_ok)

Regole campionamento	di	Nessuna
Formula		$IQ21 = (N_{ok} / N_{req}) \times 100$
Regole arrotondamento	di	Nessuna
Valore di soglia		– $IQ21 = 100\%$
Azioni contrattuali		Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento (ossia per ogni corso/modulo non conforme), l'applicazione della penale “ Non conformità dei docenti o della documentazione formativa ” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.
Applicazione		Amministrazione Contraente
Eccezioni		Sono escluse dal calcolo le sostituzioni di docenti richieste o autorizzate dall'Amministrazione.

4.22 IQ22 – Rilievi su obbligazioni contrattuali non presidiate

L'indicatore misura il numero di **rilievi formali** emessi dall'Amministrazione Contraente in relazione a **obbligazioni contrattuali non adempiute** dal Fornitore **nei tempi e/o nei modi** previsti dal Contratto Esecutivo, dal Piano di Lavoro Generale o dai relativi allegati, **non già oggetto di specifici indicatori di qualità**.

ASPETTO DA VALUTARE	NUMERO DI RILIEVI FORMALI PER INADEMPIMENTI CONTRATTUALI NON COPERTI DA ALTRI INDICATORI		
Unità di misura	Percentuale	Fonte dati	– Comunicazioni formali dell'Amministrazione – Note di rilievo – Verbali – Piano di Lavoro Generale
Periodo di riferimento	di Durata della fornitura Periodi di verifiche di conformità	Frequenza di misurazione	di Trimestrale
Dati da rilevare	– N_rilievi = numero di rilievi formali emessi nel periodo		
Regole di campionamento	Nessuna		
Formula	$IQ22 = N_rilievi$		
Regole di arrotondamento	Nessuna		
Valore di soglia	– $IQ22 \geq 3$		
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale inferiore al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Mancate obbligazioni contrattuali” pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.		
Applicazione	Amministrazione Contraente		
Eccezioni	Non rientrano nel calcolo i rilievi relativi a obbligazioni già sanzionate tramite altri indicatori di qualità o per cause non imputabili al Fornitore, purché documentate e accettate.		

5 SCHEMA PER LA PRESENTAZIONE DEI CURRICULA

Di seguito viene presentato lo schema che il Fornitore dovrà utilizzare per la compilazione del curriculum vitae. Si sottolinea che nella redazione dei contenuti dovranno essere privilegiati gli aspetti di interesse per la fornitura e che orientativamente il documento non dovrà superare le 3 pagine.

Nominativo	<i>(Inserire il Cognome e il Nome della risorsa)</i>		
Ruolo	<i>(Inserire il Ruolo attualmente ricoperto dalla risorsa)</i>		
Figura professionale	<i>(Indicazione del ruolo assegnato alla risorsa in funzione delle figure professionali richieste nel capitolato tecnico).</i>		
Servizio/attività	<i>(Fornire l'indicazione del servizio/attività per cui viene proposta la risorsa in relazione agli ambiti definiti nel Capitolato Tecnico)</i>		
Conoscenze	<i>(Fornire una breve descrizione del profilo professionale in termini di conoscenze/competenze e di aree chiave in cui la risorsa ha maturato esperienze significative)</i>		
Principali Esperienze Lavorative	<i>(Indicare le esperienze più significative per la gara in oggetto e comprovanti le competenze richieste nel Capitolato Tecnico, a partire dalla più recente, fornendo una breve descrizione delle attività svolte, del ruolo ricoperto, della durata del progetto. È necessario suddividere le esperienze per anno e per settore (Es: Pubblica Amministrazione, Bancario, Telecomunicazioni)</i>		
	Settore	Data inizio-Data fine	Esperienze

Classificazione Consip: Ambito Pubblico

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per l'affidamento di servizi professionali per la gestione e conduzione di infrastrutture di cybersecurity delle Pubbliche Amministrazioni (ID 2909)

Competenze Tecniche	<i>(Indicare le competenze specifiche di cui si è in possesso)</i>		
Specializzazioni	<i>(Indicare eventuali specializzazioni, master, ecc.)</i>		
	Anno	Titolo	Descrizione
Certificazioni	<i>(Indicare eventuali certificazioni)</i>		
	Anno	Titolo	Descrizione
Istruzione	<i>(indicare i titoli di studio)</i>		
Lingue	<i>Per ogni lingua straniera, indicare il grado di conoscenza, dove:</i> <i>1 -in grado di leggere</i> <i>2 - in grado di leggere e scrivere</i> <i>3 - in grado di leggere, parlare e scrivere in maniera più che comprensibile</i> <i>4 - fluente sia nello scritto che nell'orale</i> <i>5 - madrelingua - (native language)</i>		
	Lingue		Grado di conoscenza

Principali pubblicazioni	<i>(indicare le principali pubblicazioni)</i>	