Capitolato tecnico – Parte Speciale

ID 2733 - GARA A PROCEDURA APERTA AI SENSI DEL D. LGS. 36/2023 E S.M.I., PER L'AFFIDAMENTO DI UN ACCORDO QUADRO AVENTE AD OGGETTO LA FORNITURA DI SOLUZIONI PER PROTEZIONE E RESILIENZA DELLE RETI E DEI SISTEMI INFORMATIVI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI – LOTTI 2, 3, 4

Classificazione Consip: Ambito Pubblico

Indice

1 PREMESSA 5

1.1 Scopo del documento 5

1.2 Oggetto 5

2 DESCRIZIONE DELLA FORNITURA 6

2.1 Prodotti 7

2.1.1 Brand, fasce e formati tecnologici 8

2.1.2 Requisiti minimi comuni 20

2.1.3 Requisiti Lotto 2 – Gestione Perimetrale e delle Interconnessioni. 26

2.1.4 Requisiti Lotto 3 – Gestione Accessi e Risorse 35

2.1.5 Requisiti Lotto 4 – Monitoraggio degli Endpoint e Gestione Eventi 39

2.1.6 Garanzia dei prodotti 46

2.2 Servizi 46

2.2.1 Servizio di installazione e configurazione (incluso nella fornitura) 46

2.2.2 Servizio di porting policy (incluso nella fornitura) 51

2.2.3 Servizio di monitoraggio e aggiornamento software/firmware (incluso nella fornitura) 51

2.2.4 Servizio di manutenzione (opzionale) 53

2.2.5 Servizio di formazione e affiancamento (opzionale) 57

2.2.6 Servizio di supporto specialistico (opzionale) 60

3 INDICATORI DI QUALITÀ 72

3.1 IQ01 – Rispetto di una scadenza contrattuale 72

3.2 IQ02 – Adeguatezza delle figure professionali proposte per la erogazione dei servizi 74

3.3 IQ03 – Adeguatezza del personale impiegato nei ruoli contrattuali 75

3.4 IQ04 – Adeguatezza dei tempi di sostituzione delle figure professionali proposte per la erogazione dei servizi 76

3.5 IQ05 -Turnover del personale impiegato nella fornitura 77

3.6 IQ06 – Impegni assunti in offerta tecnica 78

3.7 IQ07 – Tempestività di risposta per il servizio di Service Desk 78

3.8 IQ08 – Percentuale di chiamate in ingresso perse per il servizio di Service Desk 80

3.9 IQ09 – Tempestività di risposta al disservizio 81

3.10 IQ10 – Tempestività del tempo di intervento 82

3.11 IQ11 – Tempestività del tempo di ripristino del servizio 84

3.12 IQ12 – Tempo di disponibilità del prodotti Cloud/SaaS 86

3.13 IQ13 – Tempestività della comunicazione degli aggiornamenti software/firmware e delle patch di sicurezza 88

3.14 IQ14 – Tempestività nell'installazione o applicazione degli aggiornamenti connessi a vulnerabilità 92

4 SCHEMA PER LA PRESENTAZIONE DEI CURRICULA 95

Indice delle figure e tabelle

Tabella 1 – Fasce, numero di brand e formati tecnologici – Lotto 2 13

Tabella 2 – Fasce, numero di brand e formati tecnologici – Lotto 3 15

Tabella 3 – Fasce, numero di brand e formati tecnologici – Lotto 4 19

Tabella 4 – Requisiti minimi DNSH per le appliance fisiche 23

Tabella 5 – Requisiti minimi DNSH per fornitura di prodotti SaaS....24

Tabella 6 - Requisiti funzionali minimi per tutte le fasce di NGFW 27

Tabella 7 – Requisiti funzionali minimi per tutte le fasce di WAAP 28

Tabella 8 – Requisiti funzionali minimi per tutte le fasce di SWG 29

Tabella 9 – Requisiti funzionali minimi per tutte le fasce di ZTNA 30
Tabella 10 – Requisiti funzionali minimi per tutte le fasce di CASB 31
Tabella 11 – Requisiti funzionali minimi per tutte le fasce di SEG 33
Tabella 12 - Requisiti funzionali minimi per tutte le fasce di Anti-APT 34
Tabella 13 - Requisiti funzionali minimi per tutte le fasce di NAC 36
Tabella 14 – Requisiti funzionali minimi per tutte le fasce di IAM 37
Tabella 15 – Requisiti funzionali minimi per tutte le fasce di PAM 38
Tabella 16 – Requisiti funzionali minimi per tutte le fasce di DLP 39
Tabella 17 - Requisiti funzionali minimi per tutte le fasce di EPP/EDR 40
Tabella 18 - Requisiti funzionali minimi per tutte le fasce di SPP 41
Tabella 19 – Requisiti funzionali minimi per tutte le fasce di SIEM 43
Tabella 20 – Requisiti funzionali minimi per tutte le fasce di SOAR 44
Tabella 21 - Requisiti funzionali minimi per tutte le fasce di XDR 45
Tabella 22 - Finestra di erogazione dei servizi 54
Tabella 23 – Classificazione dei Severity Code 54
Tabella 24. Esperienza aggiuntiva da considerare come “cultura equivalente” 65

1 PREMESSA

1.1 Scopo del documento

Il presente Capitolato Tecnico Speciale ha l'obiettivo di descrivere i requisiti minimi relativi ai **prodotti** e ai **servizi per la protezione e resilienza delle reti e sistemi informativi**, oggetto dei seguenti Lotti:

- **Lotto 2**: fornitura di prodotti e servizi connessi di Gestione perimetrale e interconnessioni;
- **Lotto 3**: fornitura di prodotti e servizi connessi di Gestione accessi e risorse;
- **Lotto 4**: fornitura di prodotti e servizi connessi di Monitoraggio degli end point e gestione eventi.

Se non diversamente specificato, i termini temporali espressi nel presente Capitolato sono tutti da intendersi come solari (di calendario).

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

1.2 Oggetto

I singoli Lotti 2, 3 e 4, hanno ad oggetto i seguenti prodotti:

- **Lotto 2**:
  - Next Generation Firewall (NGFW);
  - Web Application and API Protection (WAAP ex WAF);
  - Secure Web Gateway (SWG);
  - Secure Email Gateway (SEG);
  - Anti-Advanced Persistent Threat (Anti-APT);
  - Zero Trust Network Access (ZTNA);
  - Cloud Access Security Broker (CASB);
- **Lotto 3**:
  - Network Access Control (NAC);
  - Identity Access Management (IAM);
  - Privileged Access Management (PAM);
  - Data Loss Protection/Prevention (DLP);
- **Lotto 4**:
  - Endpoint Protection Platform (EPP)/Endpoint Detection & Response (EDR);
  - Server Protection Platform (SPP);

- eXtended Detection and Response (XDR);
- Security Information and Event Management (SIEM);
- Security Orchestration Automation and Response (SOAR).

Nell'ambito di ciascun Lotto, sarà richiesto in fase di gara ai concorrenti di offrire prodotti relativi a un numero fisso di brand, come meglio indicato al successivo paragrafo 2.1.1.

Tutti i Lotti hanno ad oggetto altresì i seguenti servizi connessi:

- **Servizi connessi inclusi nella fornitura (il cui prezzo si intende incluso in quello offerto per i prodotti sopra elencati)**:
  - installazione e configurazione;
  - porting policy;
  - monitoraggio e aggiornamento software/firmware;
- **Servizi connessi opzionali (per i quali sarà richiesta ai concorrenti specifica quotazione in fase di gara)**:
  - manutenzione;
  - formazione e affiancamento;
  - supporto specialistico.

Ciascuna Amministrazione potrà acquistare i Servizi connessi opzionali entro i limiti indicati al successivo paragrafo 2.2

2 DESCRIZIONE DELLA FORNITURA

Ai fini del presente Capitolato, i prodotti oggetto di fornitura possono essere resi disponibili secondo differenti **formati tecnologici di erogazione**, come indicati nelle tabelle dei singoli Lotti. I formati tecnologici sono definiti come segue.

I formati tecnologici di erogazione riflettono il modello **di distribuzione del prodotto nel suo complesso** e possono includere, a seconda della tipologia di soluzione, **componenti software installati localmente (es. agent)** e/o **componenti centralizzate di gestione (es. console)**.

1. Appliance Fisica

Prodotto fornito come **apparato hardware dedicato**, comprensivo del software di base e applicativo del produttore.

Il formato Appliance Fisica comprende:

- hardware dedicato;

- software di base e applicativo del produttore.

Esempi tipici di utilizzo includono firewall fisici o apparati di sicurezza con hardware proprietario.

2. Appliance Virtuale

Prodotto fornito come **appliance software**, da installare su infrastruttura virtuale esistente, senza fornitura di hardware fisico dedicato.

Il formato Appliance Virtuale è generalmente distribuito come pacchetto preconfigurato (ad esempio file OVA/OVF) e comprende:

- sistema operativo ottimizzato;
- applicazione di sicurezza (ad esempio firewall, proxy, IDS);
- configurazioni di base necessarie al funzionamento.

Esempi tipici di utilizzo includono firewall virtuali o altri prodotti di sicurezza installati su piattaforme di virtualizzazione (ad esempio VMware, Hyper-V o equivalenti).

3. Cloud / SaaS

Prodotto erogato come **servizio cloud**, fruibile in modalità subscription, senza fornitura di hardware o appliance software da installare presso il Committente.

Il formato Cloud/SaaS comprende:

- software applicativo;
- servizio cloud di erogazione e gestione.

Esempi tipici di utilizzo includono firewall SaaS, piattaforme di sicurezza cloud o servizi di protezione erogati integralmente tramite infrastrutture cloud.

2.1 Prodotti

Con riferimento a ciascun Lotto, ogni concorrente, dovrà offrire, per ogni prodotto **i formati tecnologici previsti** (appliance fisiche, appliance virtuali, soluzioni Cloud/SaaS **ovvero soluzioni software**, ove applicabile), in ottemperanza a quanto indicato in:

Tabella 1 – Fasce, numero di brand e formati tecnologici – Lotto 2;

Tabella 2 – Fasce, numero di brand e formati tecnologici – Lotto 3;

Tabella 3 – Fasce, numero di brand e formati tecnologici – Lotto 4.

I requisiti indicati nel presente documento in relazione ai prodotti si riferiscono a tutte tali possibili modalità. Per le sole appliance fisiche, sono date indicazioni puntuali rispetto all'hardware.

In particolare, tutti i prodotti costituiti da un apparato HW dovranno essere consegnati alle singole Amministrazioni corredati dagli alimentatori/Power Supply Unit necessari alla loro corretta alimentazione e dal necessario corredo di cavi e relativi accessori per permettere una corretta posa in opera ed installazione.

Per tutti i prodotti che vengono dimensionati su base Throughput si intende il throughput ottenuto con le funzionalità di analisi richieste, come requisiti minimi e migliorativi (se offerti), **contemporaneamente attive**.

2.1.1 Brand, fasce e formati tecnologici

Nell'ambito delle sottostanti tabelle sono indicati, in relazione a ciascun prodotto:

1. i formati tecnologici;
2. la metrica di valutazione;
3. le fasce dimensionali/prestazionali;
4. il numero fisso di brand da offrire (ossia obbligatori), per singolo prodotto, riferito a tutte le fasce;
5. il numero minimo di soluzioni da offrire per ciascun formato tecnologico, per singolo prodotto, ciascuna completa di tutte le fasce previste;
6. l'eventuale numero di soluzioni aggiuntive che il concorrente può offrire, nei formati tecnologici previsti, ai fini dell'attribuzione del relativo punteggio migliorativo., ove previsto.

Si precisa che, per ciascun prodotto, considerando complessivamente tutti i brand offerti, il concorrente deve offrire almeno il numero minimo di soluzioni indicato nelle tabelle seguenti, secondo la distribuzione prevista tra i diversi formati tecnologici. Ciascuna soluzione offerta deve essere completa di tutte le fasce dimensionali o prestazionali previste per il relativo formato tecnologico. Resta inteso che, per ciascun brand, deve essere offerta almeno una soluzione in uno dei formati tecnologici previsti. Una volta aggiudicata la gara, in fase di esecuzione contrattuale, l'Amministrazione, a seguito delle proprie valutazioni, svolte autonomamente oppure con il supporto del fornitore del Lotto 1, potrà indirizzarsi verso uno specifico brand e uno specifico formato tecnologico, tra quelli offerti dall'aggiudicatario. In particolare, la scelta del brand dovrà avvenire:

- all'esito di apposita valutazione comparativa di tipo tecnico ed economico tra le diverse soluzioni disponibili;
- nel rispetto in ogni caso dei principi di parità di trattamento, concorrenza, economicità, efficienza, tutela degli investimenti, riuso e neutralità tecnologica.

Per i prodotti Cloud/SaaS, dovranno essere rispettate le condizioni previste al paragrafo *7.3 Servizi Cloud* del Capitolato tecnico generale.

2.1.1.1 Lotto 2

LOTTO 2						
PRODOTTO	**FORMATO TECNOLOGICO**	**METRICA**	**FASCE DIMENSIONALI/ PRESTAZIONALI**	**NUMERO DI BRAND OBBLIGATORI**	**NUMERO MINIMO DI SOLUZIONI DA OFFRIRE PER FORMATO TECNOLOGICO**	**NUMERO DI SOLUZIONI AGGIUNTIVE OFFERTE NEI FORMATI TECNOLOGICI PREVISTI**
NGFW	Appliance Fisica	Throughput	– Fino a 600 Mbps – Fino a 2 Gbps – Fino a 4 Gbps – Fino a 6 Gbps – Fino a 10 Gbps – Fino a 20 Gbps – Fino a 30 Gbps – Fino a 50 Gbps	5	– 4 Appliance Fisica – 2 Appliance Virtuale – 1 Cloud/SaaS *(totale minimo=7)*	Da 1 a 5 soluzioni aggiuntive tra AF, AV, Cloud/SaaS *(totale complessivo = da 8 a 12)*
	Appliance Virtuale	Virtual CPU o Throughput	– 2 vCPU o 0,96 Gbps – 4 vCPU o 2,46 Gbps – 8 vCPU o 4,8 Gbps – 12 vCPU o 8,5 Gbps – 16 vCPU o 10,84 Gbps – 32 vCPU o 16 Gbps – 48 vCPU o 35 Gbps – 64 vCPU o 50 Gbps			
	Cloud/SaaS	Utenti	– Fino a 100 utenti – Fino a 500 utenti – Fino a 1.000 utenti – Fino a 2.000 utenti – Fino a 5.000 utenti – Fino a 10.000 utenti			

LOTTO 2						
PRODOTTO	**FORMATO TECNOLOGICO**	**METRICA**	**FASCE DIMENSIONALI/ PRESTAZIONALI**	**NUMERO DI BRAND OBBLIGATORI**	**NUMERO MINIMO DI SOLUZIONI DA OFFRIRE PER FORMATO TECNOLOGICO**	**NUMERO DI SOLUZIONI AGGIUNTIVE OFFERTE NEI FORMATI TECNOLOGICI PREVISTI**
WAAP	Appliance Fisica	Throughput	– Fino a 500 Mbps – Fino a 2,5 Gbps – Fino a 5 Gbps – Fino a 10 Gbps – Fino a 70 Gbps	4	– 1 Appliance Fisica – 3 Appliance Virtuale – 1 Cloud/SaaS *(totale minimo = 5)*	Da 1 a 4 soluzioni aggiuntive tra AF, AV e Cloud/SaaS *(totale complessivo = da 6 a 9)*
	Appliance Virtuale	Virtual CPU o Throughput	– 2 vCPU o 0,8 Gbps – 4 vCPU o 2,0 Gbps – 8 vCPU o 4,5 Gbps – 16 vCPU o 8,4 Gbps – 32 vCPU o 16,3 Gbps – 64 vCPU o 30,2 Gbps			
	Cloud/SaaS	Classi di richieste mensili **o** N. applicazioni	– 10 Mln eventi / 2 App – 50 Mln / 5 App – 250 Mln / 15 App – 1 Mld / 40 App – 5 Mld+ / App illimitate			
SWG	Appliance Fisica	Utenti	– Fino a 6.000 utenti – Fino a 20.000 utenti – Fino a 60.000 utenti	4	– 2 Appliance Fisica – 2 Appliance Virtuale – 1 Cloud/SaaS *(totale minimo = 5)*	Da 1 a 3 soluzioni aggiuntivei tra AF, AV e Cloud/SaaS *(totale complessivo = da 6 a 8)*
	Appliance Virtuale	Utenti **o** Throughput	– Fino a 6.000 utenti o 4,7 Gbps – Fino a 20.000 utenti o 13,8 Gbps – Fino a 60.000 utenti o 39,2 Gbps			
	Cloud/SaaS	Utenti	– Fino a 6.000 utenti – Fino a 20.000 utenti – Fino a 60.000 utenti			

LOTTO 2						
PRODOTTO	**FORMATO TECNOLOGICO**	**METRICA**	**FASCE DIMENSIONALI/ PRESTAZIONALI**	**NUMERO DI BRAND OBBLIGATORI**	**NUMERO MINIMO DI SOLUZIONI DA OFFRIRE PER FORMATO TECNOLOGICO**	**NUMERO DI SOLUZIONI AGGIUNTIVE OFFERTE NEI FORMATI TECNOLOGICI PREVISTI**
ZTNA	Appliance Virtuale	Utenti	– Fino a 100 utenti – Fino a 500 utenti – Fino a 1.000 utenti – Fino a 2.000 utenti – Fino a 5.000 utenti – Fino a 10.000 utenti	3	– 1 Appliance Virtuale – 2 Cloud/SaaS *(totale minimo = 3)*	1 soluzione aggiuntiva tra AV o Cloud/SaaS *(totale complessivo = 4)*
	Cloud/SaaS	Utenti	– Fino a 100 utenti – Da 101 a 500 utenti – Da 501 a 1.000 utenti – Da 1.001 a 2.000 utenti – Da 2.001 a 5.000 utenti – Da 5.001 a 10.000 utenti			
CASB	Cloud/SaaS	Utenti	– Fino a 100 utenti – Fino a 500 utenti – Fino a 1.000 utenti – Fino a 2.000 utenti – Fino a 5.000 utenti – Oltre 5.000 utenti	3	– 3 Cloud SaaS (una per ogni brand) *(unico formato previsto)*	Non previsto
SEG	Appliance Fisica	Email/ora	– Fino a 20.000 email/ora – Fino a 100.000 email/ora – Fino a 250.000 email/ora – Fino a 350.000 email/ora – Fino a 700.000 email/ora	4	– 1 Appliance Fisica – 2 Appliance Virtuale – 2 Cloud/SaaS *(totale minimo = 5)*	Da 1 a 4 soluzioni aggiuntivetra AF, AV e Cloud/SaaS *(totale complessivo = da 6 a 9)*
	Appliance Virtuale	vCPU **o** Email/ora	– 2 vCPU o 20.000 email/ora – 4 vCPU o 45.000 email/ora – 8 vCPU o 100.000 email/ora			

LOTTO 2						
PRODOTTO	**FORMATO TECNOLOGICO**	**METRICA**	**FASCE DIMENSIONALI/ PRESTAZIONALI**	**NUMERO DI BRAND OBBLIGATORI**	**NUMERO MINIMO DI SOLUZIONI DA OFFRIRE PER FORMATO TECNOLOGICO**	**NUMERO DI SOLUZIONI AGGIUNTIVE OFFERTE NEI FORMATI TECNOLOGICI PREVISTI**
			– 16 vCPU o 220.000 email/ora – 32 vCPU o 450.000 email/ora – 64 vCPU o 850.000 email/ora			
	Cloud/SaaS	Utenti	– Fino a 1.000 utenti – Fino a 5.000 utenti – Fino a 10.000 utenti – Fino a 20.000 utenti – Oltre 20.000 utenti			
Anti-APT	Appliance Fisica	File/ora	– Fino a 500 file/ora – Fino a 1.000 file/ora – Fino a 3.000 file/ora – Fino a 5.000 file/ora – Fino a 8.000 file/ora	3	– 1 Appliance Fisica – 2 Appliance Virtuale – 2 Cloud/SaaS *(totale minimo = 5)*	1 soluzione aggiuntiva tra AF, AV e Cloud/SaaS *(totale complessivo = 6)*
	Appliance Virtuale	vCPU **o** File/ora	– 2 vCPU o 100 file/ora – 4 vCPU o 400 file/ora – 8 vCPU o 800 file/ora – 16 vCPU o 2.000 file/ora – 32 vCPU o 4.700 file/ora – 64 vCPU o 10.300 file/ora			
	Cloud/SaaS	Utenti	– Fino a 1.000 utenti – Fino a 5.000 utenti – Fino a 10.000 utenti – Fino a 20.000 utenti – Oltre 20.000 utenti			

Tabella 1 – Fasce, numero di brand e formati tecnologici – Lotto 2

2.1.1.2 Lotto 3

LOTTO 3						
PRODOTTO	**FORMATO TECNOLOGICO**	**METRICA**	**FASCE DIMENSIONALI/ PRESTAZIONALI**	**NUMERO DI BRAND OBBLIGATORI**	**NUMERO MINIMO DI SOLUZIONI DA OFFRIRE PER FORMATO TECNOLOGICO**	**NUMERO DI SOLUZIONI AGGIUNTIVE OFFERTE NEI FORMATI TECNOLOGICI PREVISTI**
NAC	Appliance Fisica	Endpoint	– Fino a 100 endpoint – Fino a 1.000 endpoint – Fino a 10.000 endpoint – Fino a 25.000 endpoint – Fino a 50.000 endpoint	4	– 2 Appliance Fisica – 3 Appliance Virtuale *(totale minimo = 5)*	Da 1 a 2 soluzioni aggiuntivetra AF e AV *(totale complessivo = da 6 a 7)*
	Appliance Virtuale	Endpoint	– Fino a 100 endpoint – Fino a 1.000 endpoint – Fino a 10.000 endpoint – Fino a 25.000 endpoint – Fino a 50.000 endpoint			
IAM	Appliance Virtuale	Utenti	– Fino a 100 utenti – Fino a 500 utenti – Fino a 1.000 utenti – Fino a 2.000 utenti – Fino a 5.000 utenti – Oltre i 5.000 utenti	4	– 2 Appliance Virtuale – 2 Cloud/SaaS *(totale minimo = 4)*	Da 1 a 2 soluzioni aggiuntivetra AV e Cloud/SaaS *(totale complessivo = da 5 a 6)*
	Cloud/SaaS	Utenti	– Fino a 100 utenti – Fino a 500 utenti – Fino a 1.000 utenti – Fino a 2.000 utenti – Fino a 5.000 utenti – Oltre i 5.000 utenti			

LOTTO 3						
PRODOTTO	**FORMATO TECNOLOGICO**	**METRICA**	**FASCE DIMENSIONALI/ PRESTAZIONALI**	**NUMERO DI BRAND OBBLIGATORI**	**NUMERO MINIMO DI SOLUZIONI DA OFFRIRE PER FORMATO TECNOLOGICO**	**NUMERO DI SOLUZIONI AGGIUNTIVE OFFERTE NEI FORMATI TECNOLOGICI PREVISTI**
PAM	Appliance Fisica	Utenti privilegiati	– Fino a 99 utenti – Da 100 a 499 utenti – Da 500 a 999 utenti – 1.000 utenti e oltre	3	– 1 Appliance Fisica – 2 Appliance Virtuale – 1 Cloud/SaaS *(totale minimo = 4)*	Da 1 a 2 soluzioni aggiuntivetra AF, AV o Cloud/SaaS *(totale complessivo = da 5 a 6)*
	Appliance Virtuale	Utenti privilegiati	– Fino a 99 utenti – Da 100 a 499 utenti – Da 500 a 999 utenti – 1.000 utenti e oltre			
	Cloud/SaaS	Utenti privilegiati	– Fino a 99 utenti – Da 100 a 499 utenti – Da 500 a 999 utenti – 1.000 utenti e oltre			
DLP	Appliance Virtuale	Utenti	– Fino a 100 utenti – Fino a 500 utenti – Fino a 1.000 utenti – Fino a 5.000 utenti – Fino a 10.000 utenti – Fino a 25.000 utenti	3	– 2 Appliance Virtuale – 2 Cloud/SaaS *(totale minimo = 4)*	1 soluzione aggiuntiva tra AV o Cloud/SaaS *(totale complessivo = 5)*
	Cloud/SaaS	Endpoint	– Fino a 500 endpoint – Da 501 a 1.000 endpoint – Da 1.001 a 5.000 endpoint – Oltre 5.000 endpoint			

Tabella 2 – Fasce, numero di brand e formati tecnologici – Lotto 3

2.1.1.3 Lotto 4

LOTTO 4						
PRODOTTO	**FORMATO TECNOLOGICO**	**METRICA**	**FASCE DIMENSIONALI/ PRESTAZIONALI**	**NUMERO DI BRAND OBBLIGATORI**	**NUMERO MINIMO DI SOLUZIONI DA OFFRIRE PER FORMATO TECNOLOGICO**	**NUMERO DI SOLUZIONI AGGIUNTIVE OFFERTE NEI FORMATI TECNOLOGICI PREVISTI**
EPP/EDR	Software (Agent + Console*)	Endpoint	– Fino a 100 endpoint – Fino a 500 endpoint – Fino a 1.000 endpoint – Fino a 5.000 endpoint – Fino a 10.000 endpoint – Fino a 25.000 endpoint	3	– 3 prodotti software	Non previsto
SPP	Software (Agent + Console*)	Server	– Fino a 50 server – Fino a 100 server – Fino a 500 server – Fino a 1.000 server – Fino a 5.000 server	2	– 2 prodotti software	Non previsto
SIEM	Appliance Fisica	EPS e device gestiti	– Fino a 50 device , max 500 eps – Fino a 100 Device, max 1.000 eps – Fino a 500 device, max 5.000 eps – Fino a 1.000 device, max 10.000 eps – Fino a 2.000 device, max 20.000 eps – Fino a 4.000 device, max 40.000 eps	4	– 1 Appliance Fisica – 2 Appliance Virtuale – 1 Cloud/SaaS *(totale minimo = 4)*	Da 1 a 4 soluzioni aggiuntive tra AF, AV e Cloud/SaaS *(totale complessivo = da 5 a 8)*

LOTTO 4						
PRODOTTO	**FORMATO TECNOLOGICO**	**METRICA**	**FASCE DIMENSIONALI/ PRESTAZIONALI**	**NUMERO DI BRAND OBBLIGATORI**	**NUMERO MINIMO DI SOLUZIONI DA OFFRIRE PER FORMATO TECNOLOGICO**	**NUMERO DI SOLUZIONI AGGIUNTIVE OFFERTE NEI FORMATI TECNOLOGICI PREVISTI**
			– Fino a 5.000 device, max 50.000 eps			
	Appliance Virtuale	EPS e device gestiti	– Fino a 50 device, max 500 eps – Fino a 100 device, max 1.000 eps – Fino a 500 device, max 5.000 ep – Fino a 1.000 device, max 10.000 eps – Fino a 2.000 device, max 20.000 eps – Fino a 4.000 device, max 40.000 eps – Fino a 5.000 device, max 50.000 eps			
	Cloud/SaaS	EPS e device gestiti	– Fino a 50 device , max 500 eps – Fino a 100 Device, max 1.000 eps – Fino a 500 device, max 5.000 ep – Fino a 1.000 device, max 10.000 eps – Fino a 2.000 device, max 20.000 eps – Fino a 4.000 device, max 40.000 eps – Fino a 5.000 device, max 50.000 eps			

LOTTO 4						
PRODOTTO	**FORMATO TECNOLOGICO**	**METRICA**	**FASCE DIMENSIONALI/ PRESTAZIONALI**	**NUMERO DI BRAND OBBLIGATORI**	**NUMERO MINIMO DI SOLUZIONI DA OFFRIRE PER FORMATO TECNOLOGICO**	**NUMERO DI SOLUZIONI AGGIUNTIVE OFFERTE NEI FORMATI TECNOLOGICI PREVISTI**
SOAR	Appliance Virtuale	Utenti	– 1 utente – 2 utenti – 3 utenti – 4 utenti – 5 utenti – 6 utenti – 10 utenti	3	– 2 Appliance Virtuale – 2 Cloud/SaaS *(totale minimo = 4)*	1 soluzione aggiuntiva tra AV o Cloud/SaaS *(totale complessivo = 5)*
	Cloud/SaaS	Utenti	– 1 utente – 2 utenti – 3 utenti – 4 utenti – 5 utenti – 6 utenti – 10 utenti			
XDR	Appliance Virtuale	Numero di endpoint	– Fino a 100 endpoint – Fino a 500 endpoint – Fino a 1.000 endpoint – Fino a 5.000 endpoint – Fino a 10.000 endpoint – Fino a 25.000 endpoint	3	– 2 Appliance Virtuale – 2 Cloud/SaaS *(totale minimo = 4)*	1 soluzione aggiuntiva tra AV o Cloud/SaaS *(totale complessivo = 5)*
	Cloud/SaaS	Numero di endpoint	– Fino a 100 endpoint – Fino a 500 endpoint – Fino a 1.000 endpoint – Fino a 5.000 endpoint – Fino a 10.000 endpoint – Fino a 25.000 endpoint			

Tabella 3 – Fasce, numero di brand e formati tecnologici – Lotto 4

*La **Console** può essere erogata in **qualsiasi formato tecnologico** (Appliance Fisica, Appliance Virtuale o Cloud/SaaS).

2.1.2 Requisiti minimi comuni

Tutti i prodotti offerti per ciascun Lotto, indicati successivamente nel presente documento, devono rispettare i requisiti minimi di cui al presente paragrafo oltre a tutti quelli indicati più nel dettaglio nei successivi.

In particolare, tutti i prodotti proposti dovranno:

1. essere disponibili sul mercato al momento della scadenza per la presentazione dell'offerta. Pertanto, tutti i prodotti proposti devono essere già commercializzati o commercializzabili al momento di presentazione dell'offerta e non sono accettati prototipi;
2. per i prodotti dotati di hardware dedicato, essere nuovi di fabbrica e non ricondizionati, per cui il numero di matricola, corrispondente ai dispositivi forniti, non dovrà mai essere stato precedentemente oggetto di fatturazione verso un cliente;
3. **non** prevedere servizi e funzionalità, che non siano esplicitamente riportati nella documentazione tecnica e nella manualistica del Produttore, in grado di comunicare verso reti esterne e/o interne;
4. prevedere la possibilità di disabilitare, da parte dell'Amministratore di sistema, qualsiasi servizio o funzionalità, documentato dal Produttore, in grado di comunicare verso reti esterne e/o interne anche per funzioni gestionali e/o di aggiornamento/manutenzione, ad eccezione delle comunicazioni strettamente necessarie all'erogazione e al funzionamento del prodotto secondo il formato tecnologico offerto. Le comunicazioni non disabilitabili devono essere debitamente documentate dal Produttore, con indicazione della relativa finalità;
5. per i prodotti dotati di hardware dedicato, essere provvisti di regolare marcatura "CE", a garanzia della conformità dei prodotti alla normativa dell'Unione applicabile alla specifica merceologia;
6. per i prodotti dotati di hardware dedicato: essere conformi alla normativa vigente, nazionale ed europea, che regolamenta la loro produzione, commercializzazione ed utilizzo e rispettare, ciascuna per le singole specifiche caratteristiche e ove applicabile in relazione allo specifico prodotto, le seguenti prescrizioni in materia di sicurezza:
   - Decreto Legislativo del 19 maggio 2016 n. 86 e s.m.i., "attuazione della direttiva 2014/35/UE concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato del materiale elettrico destinato ad essere adoperato entro taluni limiti di tensione";
   - D. Lgs. 4 marzo 2014, n. 27 e s.m.i., "attuazione della direttiva 2011/65/UE sulla restrizione dell'uso di determinate sostanze pericolose nelle apparecchiature elettriche ed elettroniche" (RoHS);
   - D. Lgs. 18 maggio 2016, n. 80 e s.m.i., "modifiche al decreto legislativo 6 novembre 2007, n. 194, di attuazione della direttiva 2014/30/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla compatibilità elettromagnetica";

- D. Lgs, n. 49/2014 così come modificato da ultimo D.Lgs. n. 11 del 3 settembre 2020 e s.m.i., “Attuazione degli articoli 2 e 3 della direttiva (UE) 2018/849 relativa a pile e accumulatori e ai rifiuti di pile e accumulatori e sui rifiuti di apparecchiature elettriche ed elettroniche.
  Inoltre:
  - l’offerente
  - oppure, se diverso dall’offerente, il produttore, così come definito all’art. 4, lett. g), del D.Lgs. 49/2014;
  - oppure, sempre se diverso dall’offerente, il distributore, così come definito all’art. 4, lett. h), del D.Lgs. 49/2014;

  dovrà essere in possesso dell’iscrizione al Registro nazionale dei soggetti obbligati al finanziamento dei sistemi di gestione dei RAEE, istituito e funzionante ai sensi del regolamento 25 settembre 2007, n. 185.

2.1.2.1 DNSH

Di seguito sono indicati i requisiti minimi relativi alle schede DNSH previsti per i prodotti oggetto di fornitura. In particolare, in riferimento ai formati tecnologici minimi richiesti al paragrafo 2.1.1 e quelli eventualmente offerti come migliorativi:

- per le forniture con formato tecnologico Appliance fisica trova applicazione quanto indicato al successivo paragrafo 2.1.2.1.1;
- per le forniture con formato tecnologico Cloud SaaS trova applicazione quanto indicato al successivo paragrafo 2.1.2.1.2.

2.1.2.1.1 Scheda 3

I seguenti requisiti minimi sono coerenti con quelli "ex ante" richiesti dalla Scheda n. 3 della circolare RGS n. 22 del 14 maggio 2024.

Con riferimento alla sottostante Tabella, si precisa che:

- qualora in possesso dei requisiti di cui ai punti (1) e (2) non è necessario possedere anche i requisiti di cui ai punti successivi;
- in assenza di un'etichetta ambientale di tipo I, secondo la UNI EN ISO 14024 (punto 2), allora si ha l'obbligo possedere i requisiti di cui a tutti i punti successivi: (3), (4), (7) e (8), con la precisazione che in assenza dei requisiti al punto (3) si ha l'obbligo di rispondere al punto (3.1);
- i requisiti di cui ai punti (1) e (7) sono comunque già previsti in via obbligatoria al precedente paragrafo 2.1.2;
- la numerazione non prevede i nn. (5) e (6), in quanto trattasi di requisiti della Scheda n. 3 non pertinenti con la merceologia oggetto della presente iniziativa.

Appliance fisiche	
Ambito	**Requisiti minimi - DNSH**
DNSH	**(1)** Iscrizione alla piattaforma RAEE in qualità di produttore e/o distributore e/o fornitore
	(2) Etichetta ambientale di tipo I, secondo la UNI EN ISO 14024, ad esempio TCO Certified, EPEAT 2018, Blue Angel, TÜV Green Product Mark o etichetta equivalente
	(3) Etichetta EPA ENERGY STAR
	(3.1) Dichiarazione del produttore che attesti che il consumo tipico di energia elettrica (Etec), calcolato per ogni dispositivo offerto, non superi il TEC massimo necessario (Etec-max) in linea con quanto descritto nell'Allegato III dei criteri GPP UE

Appliance fisiche	
Ambito	**Requisiti minimi - DNSH**
	(4) Per i server e prodotti di archiviazioni dati, conformità alla seguente normativa: ecodesign (Regolamento (EU) 2019/424
	(7) Rispetto della seguente normativa: REACH (Regolamento (CE) n.1907/2006); RoHS (Direttiva 2011/65/EU e ss.m.i.); Compatibilità elettromagnetica (Direttiva 2014/30/UE e ss.m.i.)
	(8) Indicazione delle limitazioni delle caratteristiche di pericolo dei materiali che si prevede utilizzare (Art. 57, Regolamento CE 1907/2006, REACH)

Tabella 4 – Requisiti minimi DNSH per le appliance fisiche

2.1.2.1.2 Scheda 6

I seguenti requisiti minimi sono coerenti con quelli “ex ante” richiesti dalla Scheda n. 6 della circolare RGS n. 22 del 14 maggio 2024. Tali requisiti si intendono riferiti al fornitore dell’infrastruttura (centri dati e sale server) relativa a ciascuna fornitura offerta con formato tecnologico SaaS.

Con riferimento alla sottostante Tabella, si precisa che:

- qualora in possesso del requisito di cui al punto (1), non è necessario possedere anche i requisiti di cui ai punti successivi;
- qualora non in possesso del requisito (1), dovranno essere posseduti i requisiti di cui ai punti:
  - (2);
  - almeno uno tra (3), (4) e (5);
  - (6);
  - (7);
  - (8);

  Solamente nel caso in cui sia posseduto il requisito di cui al punto (5), non sarà necessario comprovare anche il possesso di cui ai precedenti punti (7) e (8).

Cloud SaaS – Servizi informatici di Hosting e cloud – Regime 2	
Ambito	**Requisiti minimi - DNSH**
DNSH	**(1)** Certificazione di sistema di gestione ambientale di tipo ISO 14001 o EMAS rilasciata sotto accreditamento.
	(2) Comunicazione del calcolo della media ponderata del potenziale di riscaldamento globale, anche per l'inventario dei refrigeranti utilizzati nei siti o per fornire il servizio, e dimostrazione dell'aderenza al metodo descritto nell'allegato IV del regolamento (UE) n. 517/2014, oppure sistema di gestione dell'energia (norma ISO 50001) o sistema di gestione ambientale (sistema EMAS o norma ISO 14001) che riportino l'uso di refrigeranti.
	(3) Svolgimento degli studi di fattibilità per l'implementazione e il rispetto di tutte le "pratiche attese" incluse nella versione più recente del codice di condotta europeo sull'efficienza energetica dei centri dati e hanno attuato tutte le pratiche attese a cui è stato assegnato il valore massimo di 5.
	(4) Adesione dei data center che ospitano i servizi di hosting e cloud alle pratiche raccomandate contenute nel CEN-CENELEC documento CLC TR50600-99-1 "Data centre facilities and infrastructures- Part 99-1 : Recommended practices for energy management".
	(5) Rispetto di tutti i Criteri dell'UE applicabili in materia di appalti pubblici verdi per i centri dati, le sale server e servizi cloud e fornite le relative prove di verifica.
	(6) Possesso per i data center che ospitano i servizi di hosting e cloud di un piano di gestione dei rifiuti.
	(7) Conformità alla seguente normativa: ecodesign (Regolamento (EU) 2019/424) considerato che la conformità alle normative può essere dimostrata anche tramite il sistema di gestione ISO 30134:2016 certificato da organismi di certificazione accreditati.
	(8) Conformità delle apparecchiature dei data center alla seguente normativa: REACH (Regolamento (CE) n.1907/2006); RoHS (Direttiva 2011/65/EU e ss.m.i.); compatibilità elettromagnetica (Direttiva 2014/30/UE). La conformità alla norma RoHS può essere dimostrata applicando la norma EN IEC 63000:2018

Tabella 5 – Requisiti minimi DNSH per fornitura di prodotti SaaS

2.1.2.2 Portabilità ed esportabilità

Tutti i prodotti offerti devono consentire all'Amministrazione, senza oneri aggiuntivi, la piena esportazione dei dati, delle configurazioni, delle policy e dei parametri operativi e di sicurezza

generati o definiti nell'ambito dell'utilizzo della soluzione, anche al termine del Contratto Esecutivo o in caso di cambio del Fornitore.

L'esportazione deve avvenire in formati aperti e standardizzati oppure comunque documentati e interoperabili, privi di dipendenze proprietarie non reversibili, in modo da consentire all'Amministrazione la consultazione e il successivo utilizzo delle informazioni esportate e da agevolarne il trasferimento verso un'altra soluzione.

Il Fornitore deve rendere disponibile la documentazione tecnica necessaria all'utilizzo delle funzionalità di esportazione. Le predette funzionalità e la relativa documentazione devono essere mantenute disponibili e aggiornate per tutta la durata della fornitura del rispettivo prodotto.

2.1.3 Requisiti Lotto 2 – Gestione Perimetrale e delle Interconnessioni.

Nel presente paragrafo sono descritti i requisiti minimi dei prodotti oggetto del Lotto 2.

2.1.3.1 Requisiti dei Next Generation Firewall (NGFW)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi ai **NGFW**.
I NGFW sono apparati che consentono l'ispezione dei pacchetti di rete e si differenziano dai firewall "tradizionali" in quanto non si occupano solamente di analizzare e filtrare i pacchetti dati sulla base della porta e/o protocollo, ma consentono di eseguire l'ispezione a livello applicativo, fornendo inoltre funzionalità di prevenzione dalle intrusioni, analisi e rilevamento dei malware e capacità di utilizzo di sorgenti esterne a supporto della propria attività di protezione.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

NGFW - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Funzionalità di network firewall (statefull inspection, policy enforcement, packet filtering, DNAT e SNAT, VPN IPSEC client to site e site to site, VPN TLS).
Funzionalità di intrusion prevention system per il rilevamento, blocco e tracciamento delle minacce, attraverso l'adozione di meccanismi di ispezione dei malware di tipo signature based, anomaly detection (es. individuazione delle anomalie nei protocolli comunemente utilizzati nell'ambito delle reti IP), analisi euristica o comportamentale (adottata per riconoscere minacce per le quali non sono state già definite le firme), con possibilità di creare anche signature personalizzate per contrastare attacchi ancora non censiti.
WEB/URL Filtering statico e dinamico, con possibilità di controllare le statistiche sulla navigazione, di bloccare l'accesso a particolari siti e creare anche categorie personalizzate.
Funzionalità anti-malware sia su base firma che su base comportamentale.
Funzionalità di anti-botnet.
Deep packet inspection per scansionare l'intero payload dei pacchetti.
TLS/SSL inspection per l'ispezione del traffico cifrato.
SSH inspection.
Controllo delle applicazioni con blocco dell'esecuzione in funzione della configurazione impostata dall'Amministratore di Sistema.
QoS bandwidth management con la possibilità di impostare una larghezza di banda minima garantita e un limite massimo di larghezza di banda per il traffico insieme ad un valore di priorità

NGFW - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Trasmissione di eventi e log al SIEM o ad altro strumento di raccolta log, ove disponibile, dell'Amministrazione.
Produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.
Supporto IPv6.
Supporto per configurazione in alta affidabilità.
Funzionalità di accesso selettivo alle applicazioni con modello Zero Trust basata su identificazione dei dispositivi client e autenticazione degli utenti.
Analisi del traffico su base geolocalizzazione degli IP e possibilità di filtraggio/blocco.

Tabella 6 - Requisiti funzionali minimi per tutte le fasce di NGFW

2.1.3.2 Requisiti del Web Application and API Protection (WAAP)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi al **WAAP**.

I WAAP sono l'evoluzione del Web Application Firewall. Questi sono progettati per proteggere le applicazioni web e le API da un'ampia gamma di attacchi informatici, analizzando il traffico sia in entrata che in uscita.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

WAAP - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Capacità di protezione dagli attacchi applicativi almeno OWASP TOP 10 (ultima versione disponibile alla data di presentazione offerta).
~~Ispezione del traffico FTP e delle versioni sicure da esso derivanti.~~
Ispezione Traffico HTTP/HTTPS.
Protezione delle API web che utilizzano formati strutturati quali JSON e XML, mediante l'analisi dei dati veicolati da questi formati.
Controllo dell'IP Reputation.
Mitigazione degli attacchi tramite reti di bot.
Possibilità di definire BlackList e Whitelist di accesso, anche basandosi sulla georeferenziazione degli IP address.
Capacità di rilevamento e mitigazione di attacchi DDOS di tipo applicativo.
SSL Offloading.

WAAP - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Supporto del protocollo IPV6.
Supporto per configurazione in alta affidabilità.
~~Dashboard di monitoraggio in tempo reale con funzionalità drill-down almeno per: Attacchi, Sessioni, dati Geografici di accesso.~~
Funzionalità di reportistica attraverso dashboard e API che consenta: - il monitor in real-time; - la realizzazione di report tramite template predefiniti o personalizzabili; - la possibilità di esportare i report.
Fornire funzionalità di Virtual Patching.
Supporto standard PCI DSS.
~~Funzionalità di Data Loss Prevention.~~
Possibilità di interrogare la base dati della soluzione tramite API.
Funzionalità di bilanciamento di livello 7 (modello ISO/OSI) delle Applicazioni.
~~Possibilità di interrogare la base dati della soluzione tramite API.~~
Implementazione di regole e policy personalizzate su base richiesta della PA.

Tabella 7 – Requisiti funzionali minimi per tutte le fasce di WAAP

2.1.3.3 Requisiti del Secure Web Gateway (SWG)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi al **SWG**.
Il SWG è una soluzione che consente di proteggere gli utenti dalle minacce derivanti dalla loro navigazione su Internet (download di malware, attacchi informatici…) e di far rispettare agli stessi la compliance aziendale (evitando ad esempio l'accesso a categorie di siti o siti specifici che violano le policy aziendali o che costituiscono una minaccia considerando i relativi contenuti).

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

SWG - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Funzionalità: - proxy del traffico in modalità trasparente ed esplicita; - capacità di filtraggio delle URL; - capacità di filtraggio dei contenuti; - capacità di filtraggio dei protocolli, tra cui HTTP/HTTPS/FTP/FTPS/SFTP; - capacità di filtraggio delle applicazioni.
Definizione criteri di sicurezza/filtraggio per utente e/o gruppi e definizione di blacklist/whitelist.

SWG - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
La soluzione dovrà supportare il reindirizzamento esplicito del traffico verso il servizio SWG mediante PAC file o mediante meccanismi equivalenti di traffic steering nativamente supportati dalla soluzione. Qualora venga utilizzato un PAC file, dovranno essere previsti: - meccanismi di limitazione degli accessi in scrittura; - trasmissione protetta mediante HTTPS. Qualora vengano adottati meccanismi alternativi al PAC file, il Fornitore dovrà garantire un livello di sicurezza almeno equivalente per quanto riguarda la protezione dell'integrità della configurazione e delle informazioni utilizzate per il reindirizzamento del traffico.
Web/URL Filtering basato su un insieme ampio e articolato di categorie predefinite (almeno 80), con possibilità di definire categorie personalizzate e di classificare o riclassificare tempestivamente URL e domini in funzione dell'evoluzione delle minacce.
Identificazione dei comportamenti potenzialmente pericolosi, blocco dei siti potenzialmente malevoli o categorizzati come tali e blocco dei file in base all'estensione.
Presenza di un database di identificativi degli attacchi e delle categorie dei siti (es. SaaS, Piattaforme Streaming, etc...). Questo deve poter essere costantemente aggiornabile anche in base a richieste specifiche della PA.
Funzionalità di protezione Anti Malware, WEB/IP reputation e anti-botnet sul traffico gestito.
Identificazione attacchi di tipo zero-day.
Applicazione delle policy definite anche ai dispositivi offnet. Per tale funzionalità potrà essere previsto l'utilizzo di agent da installare sui dispositivi remoti e che supporti i principali Sistemi Operativi (Windows, MacOS, iOS, Android).
Supporto di alcuni dei principali meccanismi di autenticazione e federazione delle identità, quali Kerberos, LDAP, integrazione con Active Directory, SAML, OIDC, OAUTH2.
Funzionalità di reportistica attraverso dashboard e API che consenta: - il monitor in real-time; - la realizzazione di report tramite template predefiniti o personalizzabili; - la possibilità di esportare i report.
Supporto del protocollo IPv6.
Supporto per configurazione in alta affidabilità.
Funzionalità di SSL/TLS Inspection.
Console di gestione centralizzata per configurazione e implementazione delle policy e controllo degli agent.

Tabella 8 – Requisiti funzionali minimi per tutte le fasce di SWG

2.1.3.4 Requisiti del Zero Trust Network Access (ZTNA)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi a **ZTNA**.

La ZTNA è una soluzione che consente agli utenti in remoto di accedere in modo sicuro alle applicazioni interne. Si basa su un modello di fiducia adattativo, dove l'attendibilità, o trust, non è mai implicita, e l'accesso viene concesso solo a ciò che è strettamente necessario, secondo il principio dei privilegi minimi e in base a policy granulari aziendali.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

ZTNA - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Garantire in modo trasparente l'accesso alle sole risorse aziendali a cui l'utente è stato autorizzato, su base profilatura.
Garantire almeno un metodo di autenticazione forte (SAML, MFA, etc…).
Supporto dei protocolli: FTP, SSH, RDP, SSL, HTTP/HTTPS, etc…).
Monitorare e valutare la postura dell'end-point sulla base di specifici criteri anche richiedibili dalla PA (a titolo esemplificativo: tipo e versione Sistema Operativo, tipo e versione del browser, anti-virus aggiornato, geolocalizzazione).
Possibilità sia di installazione di agent su dispositivo, sia la possibilità di accesso clientless (agentless) via browser.
Supporto dei principali Sistemi Operativi (Windows, Linux, macOS).
Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti o personalizzabili; - la possibilità di esportare i report.
Supporto del protocollo IPv6.
La soluzione deve garantire la gestione delle policy di accesso alle risorse aziendali (infrastrutture, dati e applicazioni), personalizzabili in base alle esigenze della PA, in contesti on-prem, cloud e ibridi.
Supporto per configurazioni in alta affidabilità.
Fornire meccanismi di protezione dalle minacce (malware, phishing, zero-day, etc…).

Tabella 9 – Requisiti funzionali minimi per tutte le fasce di ZTNA

2.1.3.5 Requisiti del Cloud Access Security Broker (CASB)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi al **CASB**.
Il CASB è una soluzione per l'identificazione dei gap di sicurezza di un'azienda nell'utilizzo dei servizi in cloud. Un CASB si colloca pertanto tra gli utenti e il cloud per monitorare e verificare che i servizi utilizzati siano a tutti gli effetti conformi con le policy di sicurezza aziendali, ed intervenire qualora venissero rilevate delle criticità.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

CASB - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Garantire almeno un metodo di autenticazione forte basato su SAML o altro metodo di riconoscimento (MFA).
Monitorare la postura di sicurezza dei dispositivi connessi permettendo il blocco degli accessi in situazioni di potenziale compromissione.
Funzionalità di Data Loss Prevention (DLP).
Monitoraggio degli utenti connessi alle applicazioni SaaS indipendentemente dai dispositivi utilizzati.
Monitoraggio continuo e analisi del comportamento utente anche in base a dati storici ad esso relativo (geolocalizzazione, IP, fasce orarie, etc…).
Garantire la gestione delle policy di accesso alle applicazioni cloud aziendali predefinite e personalizzabili in base alle esigenze della PA (es. geolocalizzazione, IP, fasce orarie, permessi di accesso alle risorse, etc…) in maniera trasparente per l'end user.
Supporto per configurazioni in alta affidabilità.
Supporto del protocollo IPv6.
Possibilità di installazione di agent su dispositivo e la possibilità di accesso clientless (agentless) via browser per supportare architetture BYOD.
Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti o personalizzabili (C-level, Compliance, Alert, Shadow IT, etc...); - la possibilità di esportare i report.
Analisi del contenuto e delle attività svolte sulle applicazioni SaaS, incluse Microsoft 365 OneDrive, Sharepoint, Teams, permettendo la rilevazione di minacce.
Rilevazione di tutte le applicazioni cloud aziendali, permettendo l'identificazione di Shadow IT.
Implementazione di meccanismi di allarmistica per segnalare eventi potenzialmente pericolosi (comportamenti anomali, dispositivi compromessi, applicazioni non autorizzate, etc…) permettendo la configurazione dei parametri da parte della PA.
Meccanismi di protezione dalle minacce (malware, phishing, zero-day, etc…).
Accesso alle risorse aziendali sulla base della profilatura utente.

Tabella 10 – Requisiti funzionali minimi per tutte le fasce di CASB

2.1.3.6 Requisiti del Secure Email Gateway (SEG)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi al **SEG**.
Un Secure Email Gateway (SEG) è una soluzione di sicurezza avanzata progettata per proteggere le comunicazioni aziendali via email. Attraverso sofisticati sistemi di filtraggio, il SEG blocca spam, phishing, malware e altre minacce informatiche prima che raggiungano la casella di posta dei destinatari. Garantisce così un ambiente di lavoro sicuro, riducendo il rischio di attacchi e proteggendo i dati sensibili aziendali.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

SEG - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Supporto al Mail Transfer Agent.
Funzionalità di protezione a più livelli per l'individuazione dello SPAM e la rilevazione di minacce attraverso più meccanismi quali l'analisi approfondita del contenuto delle email e il filtraggio delle URL presenti nel corpo del messaggio.
Funzionalità di anti-virus, anti-phishing, anti-BEC, anti-spoofing, Cousin Domain Detection, anti-spam e anti-malware in grado di identificare virus, worms, ransomware attraverso il riconoscimento di signature e analisi euristica dei contenuti.
Protezione da email massive e di marketing.
Protezione realtime attraverso API o SMTP relay.
Identificazione di attacchi di tipo zero-day.
Blocco email in base alla lingua utilizzata o specifici charset.
Rimozione, tramite l'analisi del contenuto dell'email e degli allegati, di file malevoli. Identificazione, tramite analisi di tipo true file type, della tipologia di file e inclusione URLs potenzialmente pericolosi.
Trattamento delle email per quali è stato identificato un virus/malware con varie opzioni quali l'invio di una notifica, la quarantena, l'eliminazione del messaggio, l'inserimento in white/black list.
Supporto dei filtri basati sulla reputazione dell'indirizzo IP di provenienza e/o URL.
Ispezione sulla posta in uscita e in ingresso.
Crittografia dei messaggi in uscita con protocollo SSL/TLS.
Supporto dell'autenticazione tramite LDAP/AD.
Aggiornamenti costanti delle signature attraverso feed di threat intelligence.
Possibilità di bloccare allegati e/o contenuti attivi nelle mail (es. MACRO). La soluzione deve segnalare all'amministrazione/utente l'avvenuto blocco.

SEG - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
La soluzione deve avere funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti e personalizzabili; - la possibilità di esportare i report.
Supporto del protocollo IPv6.
Supporto per configurazione in alta affidabilità.
Supporto dei protocolli SPF, DKIM o in alternativa del protocollo DMARC.
Cifratura automatica dei messaggi in uscita per i quali risultano verificate delle politiche di identificazione configurabili (policy based encryption).
Identificazione di immagini potenzialmente dannose.
Creazione di regole di spam personalizzate.
Identificazione di testo nascosto all'interno di immagini presenti nelle email.
Possibilità di interrogare la base-dati della soluzione tramite API.
Funzionalità di Data Loss Prevention nell'ispezione delle mail in uscita almeno attraverso l'identificazione di parole chiave o pattern di dati.
Supporto alla segnalazione delle mail sospette di spam attraverso meccanismi di semplificazione della segnalazione da parte degli utenti.

Tabella 11 – Requisiti funzionali minimi per tutte le fasce di SEG

2.1.3.7 Requisiti dell'Anti-Advanced Persistent Threat (Anti-APT)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi all'**Anti-APT**.
La soluzione di Anti-APT consente l'analisi di file che possono essere inviati all'apparato da altri dispositivi di sicurezza o direttamente dal personale preposto alla gestione della cybersecurity. All'interno dell'ambiente protetto è quindi possibile, attraverso varie tecniche, esaminare i file e i loro comportamenti per determinare se questi siano o meno malevoli, assegnando loro un grado di severità.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

Anti-APT - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Supportare ambienti di analisi basati su Sistemi Operativi Windows, MacOS e Unix-based.

Anti-APT - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Rilevazione in ambiente isolato: - mediante analisi comportamentale di malware, minacce zero-day e APT; - mediante analisi del traffico di comunicazioni C&C, botnet, worm.
Supporto di almeno le seguenti tipologie di file: .zip, .gz, .bz2, .exe, .dll, .bat, .pdf, .jar, .doc, .docx, .xls, .xlsx, .ppt, .pptx., .iso, .img.
Permettere la personalizzazione degli ambienti di analisi al fine di garantire le stesse caratteristiche (configurazioni, drivers, applicazioni installate, etc…) dell'ambiente di esercizio.
Permettere di operare in modalità interattiva e/o automatizzata.
Raccolta di screenshot di ciò che accade all'interno dell'ambiente d'analisi durante la detonazione di una sample, integrandoli nei report d'analisi.
Integrazione di regole di pattern detection, quali YARA rules, personalizzate e definite dalla PA a seconda delle necessità.
Estrazione di IoC, IoA, identificati durante l'esecuzione dell'analisi, permettendone l'export nei formati standard (STIX).
Parallelizzare più macchine virtuali per l'analisi contemporanea di più sample.
Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti o personalizzabili; - la possibilità di esportare i report che contengano tutte le attività svolte e i relativi risultati sia in termini di scoring che di indicatori quali, a titolo esemplificativo: o URLs estratti; o Processi creati a runtime; o Connessioni realizzate verso l'esterno (possibile C&C), movimento laterale, botnet, worm; o tentativi di Privilege Escalation.
Possibilità di confrontare le firme dei malware in analisi con quelle presenti nella propria base dati al fine di identificare casistiche già note. Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi Anti-APT 7.5 e 7.6, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano di identificare casistiche già note.
Meccanismi di notifica (email, trouble-ticket, etc…) quando il risultato dell'analisi evidenzia comportamenti pericolosi.
Deve essere possibile gestire la configurazione della soluzione via GUI (Graphical User Interface) o CLI (Command Line Interface).
Supporto del protocollo IPv6.
Supporto a configurazione in alta affidabilità.

Tabella 12 - Requisiti funzionali minimi per tutte le fasce di Anti-APT

2.1.4 Requisiti Lotto 3 – Gestione Accessi e Risorse

Nel presente paragrafo sono descritti i requisiti minimi dei prodotti oggetto del Lotto 3.

2.1.4.1 Requisiti dei Network Access Control (NAC)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi ai **NAC**.
Il NAC consente l'implementazione di regole per il controllo degli accessi all'infrastruttura aziendale da parte degli utenti, siano essi "umani" (attraverso personal computer, apparati mobili, …) oppure "cose" (elementi in ambito *IoT*). Le regole possono basarsi su più modalità quali l'autenticazione degli utenti, la configurazione degli apparati che accedono alla rete, il ruolo degli utenti. Per mezzo del NAC è inoltre possibile applicare regole successive alla connessione degli utenti, in base ad eventi che possono provenire da altri elementi di sicurezza.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

NAC - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Discovery degli endpoint connessi alle reti aziendali e aggiornamento dell'inventario dei dispositivi connessi, siano essi Personali, aziendali, sistemi IoT, etc...
Controllo degli accessi in base alle policy di sicurezza.
Gestione accessi Guest.
Profilatura degli endpoint di rete indipendentemente dalla modalità di accesso alla rete.
Supporto standard 802.1x, MAC Authentication, Web Authentication.
Integrazione con sistemi di Identity Management esterni: Radius/LDAP/Active Directory. Inoltre deve permettere l'utilizzo della Multi-Factor Authentication.
Assegnazione dinamica della VLAN in base a parametri di autenticazione o profilatura.
Isolamento di endpoint di rete non autorizzati.
Gestione delle regole e policy da una dashboard centralizzata.
Funzionalità di BYOD (Bring Your Own Device) almeno per endpoint Android e iOS.
Funzionalità di check compliance con agent su endpoint Windows, MacOS e Linux, con possibilità di verifica della presenza di software installati e/o file sul sistema operativo e/o software antivirus.
Visibilità dispositivi IoT.
Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti o personalizzabili; - la possibilità di esportare i report.
Supporto del protocollo IPv6.

NAC - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Supporto per configurazione in alta affidabilità.
Funzionalità Radius Server.
Profilatura degli endpoint basata su tecniche agent-less.
Implementazione di strategia Role Based Access Control e Least Privilege.
Funzionalità di creazione livelli di segmentazione della rete al fine di definire regole puntuali e adattate al segmento.
Valutazione della postura di sicurezza dei dispositivi aziendali e degli endpoint prima di permettere l'accesso alla rete.

Tabella 13 - Requisiti funzionali minimi per tutte le fasce di NAC

2.1.4.2 Requisiti dei Identity Access Management (IAM)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi agli **IAM**.
Una soluzione IAM consente di gestire il ciclo di vita end-to-end delle identità e dei diritti degli utenti per tutte le risorse aziendali (sistemi, reti e dati), sia nei data center sia nel cloud.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

IAM - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Automazione dei processi di creazione, aggiornamento periodico e rimozione delle identità e delle utenze.
Definizione e gestione dei profili e dei ruoli, specificando per ogni risorsa i privilegi d'accesso.
Garantire la definizione di policy granulari basate su attributi e informazioni di contesto.
Integrazione nativa con sistemi SSO fornendo l'accesso attraverso diverse applicazioni e servizi definibili dalla PA.
Supporto alla Multi Factor Authentication.
Funzionalità di offuscamento delle informazioni relative a login falliti e/o errori (dove risiede l'errore, etc...).
Funzionalità di definizione del ciclo di vita delle password utente (durata della password, regole di costruzione, riutilizzo, etc...).
Le password devono essere conservate e trasmesse in maniera sicura attraverso protocolli specifici e crittografia.
Garantire policy di accesso da remoto granulari per ogni singolo utente (VPN, etc...).
Implementazione di misure di logging dettagliate di tutti i tentativi di autenticazione e attività utente.
Permettere il blocco automatico dell'accesso dopo un numero di tentativi falliti personalizzabile.

IAM - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Permettere la personalizzazione delle attività di reset, sblocco e richieste d'accesso self-service anche in base al profilo/ruolo utente.
Gestione centralizzata di policy, gestione degli accessi e monitoring dello stato del sistema.
Motore di analisi del rischio per valutazione del contesto (geolocalizzazione, device, storico degli accessi).

Tabella 14 – Requisiti funzionali minimi per tutte le fasce di IAM

2.1.4.3 Requisiti dei Privileged Access Management (PAM)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi ai **PAM**.
La soluzione PAM consente di garantire l'accesso sicuro agli asset dell'organizzazione che sono considerati critici, consentendo, nel contempo, il rispetto della compliance a standard e/o processi aziendali. Attraverso la soluzione di PAM deve essere possibile: identificare gli account privilegiati sugli apparati, sistemi e applicazioni garantendone la loro gestione; controllare l'accesso a tali account privilegiati; isolare, monitorare e registrare le azioni svolte durante le sessioni effettuate attraverso gli account privilegiati; gestire e archiviare in maniera sicura le credenziali utilizzate dagli account privilegiati.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

PAM - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Gestione delle password di accesso attraverso l'utilizzo di una "cassaforte" elettronica in grado di generare password sicure in maniera dinamica.
Garantire la protezione delle password salvate attraverso protocolli sicuri di encryption.
Supporto gestione delle chiavi SSH.
Isolamento delle sessioni privilegiate.
Monitoraggio delle sessioni privilegiate in real time.
Tracciatura e registrazione delle attività dell'utente durante la sessione privilegiata, al fine di effettuare audit sulle attività effettuate (Capability to monitor, record, and control privileged sessions in real-time).
Possibilità di limitare l'accesso in base all'orario.

PAM - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Funzionalità di reportistica e logging che consentano: - il tracciamento di tutte le attività privilegiate; - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti e personalizzabili; - la possibilità di esportare i report.
Discovery automatico degli account privilegiati.
Supporto all'autenticazione di terze parti (ad es. fornitori, consulenti) che accedono da remoto.
Possibilità di utilizzare una password in real-time senza che l'utente conosca mai la password utilizzata.
Supporto IPv6.
Supporto alta affidabilità.
Possibilità di definire dei workflow per la gestione del processo autorizzativo degli accessi per gli account privilegiati.
Possibilità di effettuare un'analisi di dettaglio delle minacce informatiche per identificare, segnalare e bloccare attività privilegiate anomale, anche in funzione del loro grado di criticità.
Possibilità di limitare l'accesso sulla base della localizzazione dell'utente.
Gestione delle password anche per Machine to Machine e Application to Application.
Permettere di definire policy basate sul Least Privilege, gestendole su base ruoli, utenti o gruppi.
Garantire la corretta protezione sia delle password, sia delle sessioni (encryption, hashing, etc…).
Funzionalità di cambio password amministrativa automatico dopo ogni singolo utilizzo.

Tabella 15 – Requisiti funzionali minimi per tutte le fasce di PAM

2.1.4.4 Requisiti dei Data Loss Prevention/Protection (DLP)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi ai **DLP**.
La Soluzione DLP consente l'ispezione e la classificazione dei dati contenuti in varie fonti - quali file, mail, applicazioni - siano essi residenti sui sistemi/applicazioni oppure durante il loro trasferimento sulla rete. Essa può inoltre prevedere l'applicazione dinamica di policy e diritti di accesso ai dati gestiti.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

DLP - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Compatibilità con dispositivi di vario genere (dispositivi fissi, mobili o personali) e indipendente dal Sistema Operativo adoperato (Windows, Linux, MacOS).

DLP - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Funzionalità di Data Discovery.
Sulla base della classificazione delle informazioni e delle policy aziendali, garantire la corretta protezione dei dati gestiti dagli endpoint, a riposo o in transito (encryption, hashing, etc…).
Consentire il blocco automatico di attività che violino le policy aziendali.
Identificazione di dispositivi di memoria di massa connessi agli endpoint ed impedire che questi vengano adoperati impropriamente (estrazione dati aziendali protetti, copia di documenti non protetti adeguatamente, etc…).
Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti e personalizzabili; - la possibilità di esportare i report.
Supporto protocollo IPv6.
Supporto alta affidabilità.
Possibilità di interrogare la base dati della soluzione tramite API.
Presenza di meccanismi di notifica immediata, tramite mail o strumento definito dalla PA, all'utente e alla struttura decisa dalla PA, nel momento in cui si rilevano attività che contravvengono alle policy definite (es. invio di file classificati verso l'esterno dell'azienda o account personali non autorizzati).

Tabella 16 – Requisiti funzionali minimi per tutte le fasce di DLP

2.1.5 Requisiti Lotto 4 – Monitoraggio degli Endpoint e Gestione Eventi

Nel presente paragrafo sono descritti i requisiti minimi dei prodotti oggetto del Lotto 4.

2.1.5.1 Requisiti dell'Endpoint Protection Platform (EPP)/Endpoint Detection & Response (EDR)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi all'**EPP/EDR**.
Una soluzione EPP/EDR consente di proteggere gli endpoint di tipo client da minacce quali virus, trojan, worm, etc, bloccando le attività di applicazioni che risultino potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

EPP/EDR - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Protezione di tutti i Sistemi Operativi principalmente in uso, quali Windows, MacOS.

EPP/EDR - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Implementazione di misure di analisi continue, inclusa l'analisi statica dei file, per l'identificazione di attività anomale o maliziose sugli endpoint.
Presenza di un set di signature già presenti sulla soluzione per permettere la protezione fin dal primo utilizzo. Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi EPP/EDR 1.11 e 1.12, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano l'identificazione e la classificazione delle minacce e risultino disponibili e attive fin dalla prima installazione dell'agent.
La soluzione deve effettuare: - il blocco di azioni dannose; - la gestione della quarantena dei file; - la pulizia dell'endpoint in seguito al rilevamento di malware.
Protezione del traffico in entrata e in uscita dagli endpoint, comprensivo di controllo delle applicazioni, delle porte e dei protocolli utilizzati al fine di prevenire attacchi e intrusioni contro gli endpoint.
Capacità di impostare regole per limitare o bloccare l'accesso a supporti removibili collegati all'endpoint.
Capacità di definire policy di sicurezza attraverso le quali sia consentita l'esecuzione dei soli programmi autorizzati.
Presenza di funzionalità di reportistica attraverso dashboard e API che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti o personalizzabili; - la possibilità di esportare i report.
Supporto del protocollo IPv6.
Supporto configurazione in alta affidabilità.
Installazione Agent attraverso sistemi centralizzati di distribuzione. Il sistema centralizzato deve permettere l'enforcing delle policy di sicurezza su tutti gli endpoint.
Permettere il blocco preventivo dell'accesso a siti maliziosi o l'apertura di allegati o file sconosciuti.
La soluzione EPP/EDR deve garantire la visibilità e il controllo delle periferiche collegate agli endpoint, assicurando meccanismi di monitoraggio, applicazione di policy di sicurezza, rilevazione di utilizzi anomali e registrazione degli eventi ai fini di audit e investigazione.
Riduzione dell'impatto sulle performance dei sistemi, garantendo un utilizzo ottimale delle risorse a disposizione.

Tabella 17 - Requisiti funzionali minimi per tutte le fasce di EPP/EDR

2.1.5.2 Requisiti della Server Protection Platform (SPP)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi al **SPP**.

Una soluzione SPP consente di proteggere gli endpoint di tipo server da minacce quali virus, trojan, worm, malware, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

SPP - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Supporto ai principali Sistemi Operativi, siano essi Windows-based o Linux-Based.
Supporto agli ambienti di virtualizzazione, ad esempio VMWare, Microsoft Hyper-V etc… (per tutti gli ambienti offerti, il Fornitore dovrà indicare in offerta l'elenco delle versioni supportate).
Garantire protezione contro attacchi di livello applicativo, inclusi attacchi botnet, DDoS e altre minacce che mirano a sfruttare vulnerabilità applicative per compromettere la disponibilità, l'integrità o la riservatezza dei dati e dei servizi.
Funzionalità di reportistica e logging che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti; - la possibilità di esportare i report.
Supporto del protocollo IPv6.
Supporto alta affidabilità.
Funzionalità Antimalware signature based e tramite sistemi di analisi comportamentale. Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi SPP 2.2 e 2.7, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano l'identificazione, la rilevazione e il blocco delle minacce note, unitamente all'analisi comportamentale.
Protezione di tutti i dati memorizzati nel Server, garantendo la protezione contro attacchi tipici delle basi dati.
Funzionalità di protezione dei file di sistema critici e delle chiavi di registro da manomissioni, autorizzando le modifiche solo in accordo alle policy definite.
Riduzione all'impatto sulle performance dei sistemi, garantendo un utilizzo ottimale delle risorse a disposizione.

Tabella 18 - Requisiti funzionali minimi per tutte le fasce di SPP

2.1.5.3 Requisiti della Security Information and Event Management (SIEM)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi al **SIEM**.

La soluzione SIEM consente di raccogliere, archiviare, monitorare log e correlare eventi con l'obiettivo di identificare attacchi o violazioni di dati. Fornisce un utile strumento a supporto delle attività di indagine (sia in real time sia storiche) in risposta a incidenti di sicurezza o a supporto

dell'analisi forense o ancora a supporto della compliance a standard. Il SIEM consente di aggregare gli eventi che sono originati da una vasta gamma di elementi, tra cui apparati di sicurezza, apparati di rete, endpoint e applicazioni, tipicamente attraverso l'analisi dei log prodotti ma anche attraverso altre fonti, quali ad esempio il traffico di rete. I dati raccolti possono essere arricchiti con ulteriori dati di contesto, quali ad esempio utenti, asset, minacce conosciute e vulnerabilità riscontrate. Il SIEM effettua attività di normalizzazione delle informazioni raccolte dalle varie fonti, fornendo viste e report specifici che consentono di semplificare le attività di analisi della vasta mole di dati raccolta.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

SIEM - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Capacità di raccogliere i log/eventi generati dagli apparati, dai sistemi e dalle applicazioni, standardizzando i formati di log per l'analisi e la correlazione.
Acquisizione dei log/eventi in real time tramite parser completi già disponibili nativamente nella soluzione.
Funzionalità di sviluppo parser di normalizzazione ad hoc per sorgenti non disponibili nativamente.
Identificazione e correlazione gli eventi per effettuale la detection delle anomalie e dei potenziali incidenti di sicurezza.
Garantire la compressione e memorizzazione dei log/eventi, garantendone l'integrità e l'indicizzazione, consentendo anche l'impostazione della retention (di almeno 12 mesi).
Implementazione di regole di correlazione personalizzabili, tenendo in considerazione anche eventi provenienti da differenti sorgenti.
Prevedere la possibilità di assegnazione di ruoli interni al SIEM, permettendo l'assegnazione della gestione e risoluzione di particolari incidenti/eventi a personale specifico.
Funzionalità di reportistica che consenta: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti; - la possibilità di esportare i report; - la realizzazione di report personalizzati.
Supporto Protocollo IPv6.
Supporto per configurazione in alta affidabilità.
Funzionalità di ticketing, il sistema deve fornire la funzionalità integrata di ticketing (gestione dei ticket) e la possibilità di integrarsi con sistemi esterni di gestione di ticketing.
Prioritizzazione degli incidenti per severità e impatto, con livelli adattabili e personalizzabili al contesto della PA.

SIEM - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
~~Possibilità di mappare gli alert di sicurezza con il framework MITRE ATT&CK o tassonomia cyber dell'ACN.~~
Supporto modalità multi-tenancy.

Tabella 19 – Requisiti funzionali minimi per tutte le fasce di SIEM

2.1.5.4 Requisiti della Security Orchestation Automation and Response (SOAR)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi al **SOAR**.
Lo strumento SOAR consente di orchestrare le funzioni utili a garantire una risposta automatizzata agli incidenti di sicurezza. Il SOAR deve quindi consentire la realizzazione di workflow in seguito a determinati eventi garantendo l'integrazione con un'ampia varietà di sistemi e di applicazioni esterne con l'obiettivo di velocizzare ed efficientare le attività di gestione di risposta agli incidenti di sicurezza.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

SOAR - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Orchestrazione del processo di risposta agli incidenti di sicurezza informatici attraverso l'impiego di playbook standardizzati e automatizzati.
Il SOAR deve: - permettere la creazione, gestione ed esecuzione di workflow automatizzati (playbook) per gestire la fase di incident response; - includere playbook predefiniti out-of-the-box.
Capacità di mettere in relazione nuovi incidenti di sicurezza con incidenti già risolti, di identificare investigazioni duplicate, al fine di ridurre i tempi di indagine.
Permettere la realizzazione di workflow più o meno complessi, includendo la possibilità di realizzare operazioni condizionali o decisionali.
Funzionalità di confronto degli Indicatori di Compromissione raccolti con gli incidenti in analisi.
Raccolta di informazioni dettagliate di tutte le attività svolte all'interno dell'indagine effettuata e di tutti gli incidenti.
Supporto protocollo IPv6.
Supporto implementazione in alta affidabilità.
Disponibilità di dashboard e reportistica per ricavare ed evidenziare le metriche/livelli di servizio più significativi relativi alle procedure di incident response, misurare la loro efficacia e l'efficacia delle misure di sicurezza adottate. Possibilità di esportare la reportistica e di realizzare dei report personalizzati.

SOAR - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
La soluzione deve poter implementare l'import e l'export di Indicatori di Compromissione, anche attraverso task automatizzati o periodici.
Funzionalità di interfaccia grafica per la creazione dei playbook.
Funzionalità di gestione degli incidenti; la soluzione deve disporre di un sistema di incident management integrato che permetta di assegnare le attività a specifici utenti della piattaforma, tracciandone le attività.
Funzionalità di creazione di diversi utenti con ruoli differenziati in modo da definire la visibilità e l'accesso a specifiche aree e /o informazioni del sistema.
Implementazione di Multi Factor Authentication e l'integrazione con sistemi di gestione delle identità aziendali.
Presenza di dashboard predefinite che supportino gli analisti nella visualizzazione e gestione degli incidenti di sicurezza. Queste dashboard devono fornire una rappresentazione chiara degli indicatori di compromissione (IoC) e delle metriche chiave relative agli incidenti.
Possibilità di definire dashboard specifiche per ogni categoria di incidente definita, in modo da mettere in evidenza solo le informazioni rilevanti per tale categoria.
Capacità del SOAR di estrarre contenuti da file, binari ed email in maniera indipendente.
Supporto modalità multi-tenancy.

Tabella 20 – Requisiti funzionali minimi per tutte le fasce di SOAR

2.1.5.5 Requisiti della eXtended Detection and Response (XDR)

Nel presente paragrafo sono descritti i **requisiti minimi** relativi al **XDR**.
La soluzione XDR è uno strumento per il controllo degli endpoint, dei gateway di posta elettronica, dei servizi cloud e degli accessi. Consente di analizzare, rilevare, indagare e rispondere agli eventi di sicurezza.

Nella tabella seguente si riportano i requisiti minimi **comuni a tutti i formati tecnologici previsti e a tutte le fasce richieste**.

XDR - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Supporto ai principali Sistemi Operativi, siano essi Windows-based o Linux-Based.
Capacità di utilizzare la rete degli agent installati come sensore per rilevare comportamenti dannosi e correlare tali informazioni su più origini di telemetria con dati storici e in tempo reale.
Capacità di analizzare gli eventi correlati per determinare gli incidenti e richiedere l'intervento dell'analista solamente laddove necessario (attività bloccanti, decision making, etc…),
Funzionalità di integrazione Nativa con soluzioni di sicurezza dello stesso vendor,

XDR - TUTTE LE FASCE
REQUISITI FUNZIONALI MINIMI
Capacità di raccogliere e analizzare dati, in maniera centralizzata, da molteplici fonti, arricchendo le informazioni disponibili sull'XDR e migliorandone le capacità di rilevazione e risposta agli incidenti.
Presenza di agent per gestire almeno sistemi Windows e Linux-based.
Capacità di assegnazione ruoli e privilegi differenti quali ad esempio Amministratore, Analista, etc con differenti livelli di accesso agli incidenti e alle risorse.
Individuazione anomalie e generazione di alert tramite detection rules personalizzabili. Dovrà permettere di inoltrare queste ultime a sistemi di log management tramite protocolli sicuri (quali TLS, etc...).
Funzionalità di analisi dei dati storici necessari per la ricostruzione della timeline di un attacco e confrontare lo stato passato "sicuro" con quello attuale dell'endpoint.
Funzionalità di distribuzione automatica degli aggiornamenti di tutti gli agent.
Il sistema deve essere capace di identificare e rispondere automaticamente agli incidenti di sicurezza meno complessi e che la PA ritenga essere automaticamente risolvibili, riducendo i tempi di risposta e di potenziale danno, ma anche fornire agli analisti tutte le informazioni necessarie per una risoluzione manuale efficace, fornendo la visualizzazione dettagliata degli eventi, strumenti di analisi avanzata e suggerimenti basati sulle best practice.
~~Capacità di mapping delle tecniche e tattiche di attacco, mettendole in relazione al MITRE ATT&CK e/o a tassonomia personalizzabile dalla PA (ACN).~~
Riduzione all'impatto sulle performance dei sistemi, garantendo un utilizzo ottimale delle risorse a disposizione.
Funzionalità di reportistica e logging che consentano: - il monitor in real-time attraverso dashboard; - la realizzazione di report attraverso template predefiniti; - la possibilità di esportare i report.
Capacità di assegnare la priorità agli incidenti in base al rischio e all'impatto per concentrare gli analisti su ciò che deve essere affrontato con urgenza.
La soluzione deve consentire la rilevazione e il blocco di minacce sulla base di signature note (signature based). Il requisito può essere soddisfatto anche mediante le funzionalità oggetto dei criteri migliorativi XDR 5.7, 5.10 e 5.12, ove offerte, purché le stesse, singolarmente oppure in combinazione, consentano la rilevazione e il blocco delle minacce note.
Funzionalità di creazione di regole di gestione (anche per singolo endpoint/asset) che la PA vuole tenere sotto controllo.
Supporto modalità multi-tenancy.

Tabella 21 - Requisiti funzionali minimi per tutte le fasce di XDR

2.1.6 Garanzia dei prodotti

Tutti i prodotti offerti dovranno prevedere una garanzia di 12 mesi dalla rispettiva "*Data di accettazione*".

Nel corso del periodo di garanzia, il Fornitore, a proprio carico, dovrà garantire la sostituzione del prodotto, ovvero la correzione di bachi software, nel caso di vizi del prodotto, di produzione o di conformità, già presenti al momento della consegna o che si manifestino, anche in seguito, durante il periodo di garanzia.

In aggiunta a tale garanzia, sia per il periodo successivo, sia per il periodo contestuale alla validità della stessa, l'Amministrazione potrà richiedere il servizio di manutenzione opzionale, per il quale dovranno essere garantiti gli SLA di cui al successivo paragrafo 2.2.4.

2.2 Servizi

Nel presente paragrafo sono descritti i servizi connessi inclusi nella fornitura e quelli opzionali, oggetto di tutti i Lotti della presente iniziativa.

Il Fornitore dovrà garantire che tutti i servizi prestati siano espletati da personale qualificato, che abbia le idonee competenze in base alle particolari attività richieste e tecnologie utilizzate.

I servizi opzionali di seguito descritti (manutenzione, formazione e affiancamento, supporto specialistico) dovranno essere acquistati contestualmente ai prodotti e dovranno essere indicati dalle Amministrazioni Contraenti fin dal Piano dei Fabbisogni. Trovano altresì applicazione i seguenti limiti:

a) qualora il valore complessivo dei prodotti oggetto del Contratto Esecutivo sia pari o inferiore a € 36.000,00 iva esclusa il valore complessivo dei servizi connessi opzionali dovrà essere pari o inferiore a € 12.000,00 iva esclusa;
b) qualora il valore complessivo dei prodotti oggetto del Contratto Esecutivo sia superiore a € 36.000,00 iva esclusa il valore complessivo dei servizi connessi opzionali dovrà essere pari o inferiore al 30% del valore del Contratto Esecutivo.

2.2.1 Servizio di installazione e configurazione (incluso nella fornitura)

Il servizio di installazione e configurazione è obbligatorio ed il relativo costo è da intendersi compreso nei corrispettivi previsti per i prodotti offerti.
Con riferimento alle forniture erogate in formato Cloud/SaaS o come soluzioni software (ad es. prodotti composti da agent e console), il servizio di installazione e configurazione si intende riferito alle attività di attivazione del servizio, provisioning, configurazione iniziale, integrazione con i sistemi dell'Amministrazione e messa in esercizio della soluzione.
Le attività, i deliverable e le relative tempistiche dovranno essere indicate nel Piano di lavoro generale.

Il servizio comprende tutto quello che è necessario per le attività di installazione e configurazione delle soluzioni acquistate dall'Amministrazione Contraente, inclusi eventuali elementi offerti come migliorativi dal Fornitore Aggiudicatario in sede di gara.
Si precisa che tutte le eventuali attività propedeutiche all'installazione degli apparati sono a carico dell'Amministrazione Contraente (predisposizione delle linee di alimentazione, linee dati, rack, supporti, predisposizione macchina per installazione software/appliance virtuali, etc…). In particolare, nel Piano dei Fabbisogni ciascuna Amministrazione dovrà fornire all'Aggiudicatario tutte le specifiche di installazione.

A titolo esemplificativo e non esaustivo dovranno essere previste almeno le seguenti attività:

- alloggiamento ed eventuale fissaggio sullo specifico supporto che sarà messo a disposizione dall'Amministrazione Contraente (rack, ripiano, …) in relazione alla tipologia di apparato (solo per apparati dotati di Hardware);
- collegamento alla rete di alimentazione, presso il punto di presenza della rete indicato dall'Amministrazione. I cavi di alimentazione si intendono inclusi nell'offerta (solo per apparati dotati di Hardware);
- collegamento alla rete dati, presso il punto di presenza della rete indicato dall'Amministrazione Contraente. I cavi per i collegamenti dati si intendono inclusi nell'offerta (fino ad una lunghezza massima di tre metri) (solo per apparati dotati di Hardware);
- configurazione dell'elemento per il suo corretto riconoscimento e funzionamento, quali:
    - configurazione dell'indirizzamento IP;
    - assegnazione del nome di rete;
    - configurazione delle policy di sicurezza;
    - creazione di utenze e profili definiti;
    - installazione del software, configurazione e attivazione delle eventuali licenze necessarie;
    - la configurazione delle specifiche funzionalità previste in base alla tipologia di elemento installato e alla complessità del sistema nel suo complesso;
    - hardening in fase di prima installazione.

I prodotti devono essere consegnati unitamente alla rispettiva manualistica tecnica d'uso (hardware, se presente, e software). I prodotti consegnati, una volta installati e configurati, saranno oggetto di apposito verbale di consegna sottoscritto tra Fornitore e Amministrazione.
Tutti i prodotti oggetto del singolo Contratto Esecutivo dovranno essere installati e configurati, e quindi pronti all'uso, entro i tempi indicati nel Piano di Lavoro Generale, che comunque non possono superare i termini di seguito indicati come eventualmente migliorati in offerta tecnica:

- **60 giorni solari, ovvero 50 giorni solari qualora sia stato offerto il relativo miglioramento in sede di gara.** decorrenti dall'approvazione del Piano di Lavoro Generale medesimo nei casi di progetti che coinvolgono fino a 10 sedi;

- **120 giorni solari, ovvero 100 giorni solari qualora sia stato offerto il relativo miglioramento in sede di gara,** decorrenti dall'approvazione del Piano di Lavoro Generale nei restanti casi.

Si precisa che i giorni sopra indicati, riguardano anche le attività di eventuale consegna delle appliance fisiche e di Porting Policy (cnf. par. 2.2.2).
Il verbale di consegna dovrà comprovare l'avvenuta esecuzione di tutte le attività inerenti la fornitura, l'installazione e la configurazione. Tale documento dovrà riportare la data di completamento della fornitura e tutte le informazioni di dettaglio qualificanti l'oggetto della fornitura stessa (ad esempio, a titolo esemplificativo e non esaustivo: l'elenco di prodotti e servizi forniti, il luogo di fornitura, il codice di riferimento dell'Ordinativo di fornitura, ecc.).

A questo punto, l'Amministrazione procederà al collaudo dei prodotti, con le modalità riportate all'interno del Piano di Lavoro Generale e tenuto conto di quanto previsto al successivo paragrafo 2.2.1.2.
Si precisa che ciascuna delle attività di consegna, installazione, configurazione e collaudo dovrà avvenire contestualmente su tutti i prodotti acquistati, salvo diversa indicazione dell'Amministrazione concordata con il Fornitore e sancita nel Piano di Lavoro Generale (es. caso in cui nel Piano di Lavoro Generale sia prevista l'effettuazione di rilasci successivi in caso di forniture di particolare complessità, o in base a manifestate esigenze), fermi restando i limiti massimi, per l'installazione e configurazione, sopra indicati.

2.2.1.1 Ritiro

Nell'ambito del servizio di installazione e configurazione, con riferimento alle sole Appliance fisiche, il Fornitore dovrà inoltre prestare l'attività di ritiro per lo smaltimento dei materiali e delle apparecchiature sostituite già in possesso dell'Amministrazione Contraente e dichiarate non più utilizzabili. L'attività è limitata ai materiali e alle apparecchiature dismesse nell'ambito del perimetro di intervento relativo all'installazione delle nuove apparecchiature (per tali intendendosi le sole appliance fisiche, escludendo quindi i casi di acquisto di appliance virtuali e SaaS), sebbene tale vincolo non implichi una corrispondenza unitaria tra un apparato nuovo e un apparato da dismettere (come ad esempio nel caso in cui una nuova appliance eroghi con un solo apparato funzionalità precedentemente erogate da più apparati).

Non si potrà procedere al collaudo dei nuovi prodotti installati finché l'Aggiudicatario non abbia provveduto a rimuovere dai locali dell'Amministrazione Contraente tutto il materiale che è stato sostituito.

In particolare, il Fornitore dovrà gestire/organizzare la raccolta, il trasporto, il trattamento adeguato, il recupero e smaltimento dei R.A.E.E. professionali secondo quanto previsto dagli artt. 13 e 24 del D.Lgs. 14 marzo 2014, n. 49, dal D.Lgs 152/2006 e s.m.i.

Resta peraltro inteso che è estranea all'oggetto dell'Accordo Quadro la fase prodromica della dismissione, che è a carico di ciascuna singola Amministrazione (es.: "verbale di fuori uso" dell'U.T.E., ecc.).
A proposito della procedura di rimozione e dismissione dei beni mobili di proprietà dello Stato, si rimanda a quanto disciplinato dalla Ragioneria Generale dello Stato, rispettivamente nella circolare n. 43 del 12 dicembre 2006 (riferimenti in materia di gestione di beni durevoli di valore non superiore a Euro 500,00 e procedura di ammortamento con relative aliquote annue), nella circolare n. 33 del 29 dicembre 2009 (Cessione dei beni mobili ai fini di : i) vendita; ii) cessione gratuita; iii) dismissione e smaltimento) e nella circolare n. 4 del 26 gennaio 2010.
Il ritiro in oggetto riguarda esclusivamente i RAEE per il loro trasporto e trattamento in conformità e nel rispetto di quanto stabilito dalle predette vigenti disposizioni normative.
Riguardo alle attività di ritiro dei rifiuti di pile e accumulatori, dovranno essere osservate le disposizioni di cui al D.Lgs. 188/2008 e s.m.i.

In ogni caso, dovranno essere osservate le previsioni normative di settore applicabili in relazione alle attività svolte.

2.2.1.2 Collaudo

Nel Piano di Lavoro Generale dovrà essere inserita un'apposita sezione, denominata Piano di Collaudo, contenente l'indicazione di tutte le prove, i test, i deliverable, e tutte le informazioni di dettaglio necessarie per la presa in carico delle forniture da parte dell'Amministrazione. Inoltre, il Piano di Collaudo dovrà prevedere un insieme minimo di verifiche tecniche di sicurezza documentate, comprensive di hardening della configurazione di default, vulnerability assessment sulla versione consegnata, verifica di gestione delle credenziali e dei log, cifratura dei dati a riposo e in transito.

Per le forniture erogate in formato Cloud/SaaS e per le soluzioni software, fermo restando quanto previsto in via generale per il collaudo, il collaudo iniziale consiste nella verifica funzionale e operativa della corretta attivazione del servizio o della soluzione, della configurazione effettuata e dell'accessibilità delle funzionalità previste, secondo quanto definito nel Piano di Collaudo.
Il Collaudo sarà svolto dalle Amministrazioni nel rispetto di quanto stabilito dall'art. 116, comma 2 e dagli artt. 36 e seguenti dell'Allegato II.14 del Codice e dei provvedimenti attuativi ivi richiamati.

L'Amministrazione Contraente, dopo l'installazione e configurazione, procederà al Collaudo delle soluzioni e potrà, a tal fine, a suo insindacabile giudizio:

– eventualmente avvalersi di apposita autocertificazione rilasciata ai sensi del D.P.R. 445/2000 dall'Aggiudicatario a seguito dell'effettuazione da parte del medesimo delle prove e dei test indicati nel Piano di Collaudo. In questo caso l'Amministrazione Contraente sottoscriverà, entro

15 giorni dalla data di acquisizione dell'autocertificazione, un "*Verbale di Collaudo*", la cui data sarà ritenuta quale "*Data di Accettazione*" della fornitura;

– provvedere essa stessa al Collaudo dei prodotti. In questo caso la verifica dovrà essere avviata entro **15 giorni** dal verbale di installazione e configurazione. L'Aggiudicatario dovrà collaborare, con mezzi, materiali e personale specializzato proprio, al supporto dei lavori dell'Amministrazione. In particolare, l'Aggiudicatario dovrà supportare l'esecuzione dei test ed il rilascio in esercizio dell'hardware (se previsto) e del software. I lavori di Collaudo dovranno concludersi positivamente nei **15 giorni** successivi all'avvio delle rispettive attività.

Resta fermo in ogni caso quanto previsto al paragrafo 2.2.1.1.

In caso di esito negativo del Collaudo, l'Aggiudicatario dovrà procedere ad ogni attività necessaria all'eliminazione dei malfunzionamenti e sostituzioni di parti e comunicare la disponibilità ad una seconda verifica entro il termine perentorio di **15 giorni** decorrenti dalla data di comunicazione dell'esito negativo del primo Collaudo, pena l'applicazione delle penali indicate negli indicatori di Qualità.

Qualora anche il secondo Collaudo abbia esito negativo, è facoltà dell'Amministrazione dichiarare risolto di diritto il Contratto Esecutivo, in tutto o in parte.

Tutte le attività di verifica dovranno concludersi con la stesura di un "*Verbale di Collaudo*". Nel caso di esito positivo, la data del "*Verbale di Collaudo*" positivo avrà valore di "*Data di accettazione*" della fornitura.

Con riferimento al Collaudo iniziale, si precisa che:

- qualora il Collaudo avvenga contestualmente su tutti i prodotti oggetto del Contratto Esecutivo, la "*Data di accettazione*" della fornitura, a decorrere dalla quale, fermo restando quanto previsto in relazione a ciascun servizio nei successivi paragrafi in relazione alla decorrenza, saranno avviati i servizi, coinciderà con la data del "*Verbale di Collaudo*" omnicomprensivo;
- qualora il Collaudo non avvenga contestualmente su tutti i prodotti oggetto del Contratto Esecutivo, ciascun prodotto avrà la sua "*Data di accettazione*" della fornitura e, fermo restando quanto previsto in relazione a ciascun servizio nei successivi paragrafi in relazione alla decorrenza, i servizi connessi inclusi nella fornitura, e quelli opzionali eventualmente richiesti (ivi compresa la rispettiva remunerazione), saranno avviati progressivamente in relazione ai relativi prodotti di volta in volta oggetto di accettazione.

L'Aggiudicatario dovrà supportare, fornendo la strumentazione e il personale necessario per la realizzazione delle prove, l'Amministrazione Contraente nell'esecuzione di tutte le verifiche funzionali previste dalle procedure che saranno concordate con l'Amministrazione stessa e definite nel Piano di Collaudo, contenuto nel Piano di Lavoro Generale. A tal fine potrà essere previsto anche l'utilizzo

di un “test-bed” da realizzarsi presso l’Amministrazione o presso locali messi a disposizione del Fornitore (su richiesta ed approvazione dell’Amministrazione).

Con riferimento alle forniture erogate con formato tecnologico SaaS:

- le stesse, e la rispettiva remunerazione, decorreranno dalla rispettiva “Data di Accettazione della Fornitura” conseguente al Collaudo iniziale di cui al presente paragrafo, ~~e avranno una durata di 36 mesi~~ *e avranno la durata determinata dall’Amministrazione, fino a un massimo di 36 mesi*;
- in relazione alle stesse saranno svolte, con le modalità indicate nel presente paragrafo, verifiche in corso di esecuzione. Nel Piano di Collaudo saranno precisate le rispettive tempistiche in coerenza con la tempificazione dei canoni e le indicazioni dell’Amministrazione relative alla fatturazione.

Le tempistiche di cui al presente paragrafo potranno essere modificate, d’accordo tra le parti, mediante espressa indicazione all’interno del Piano di Collaudo.

2.2.2 Servizio di porting policy (incluso nella fornitura)

Il servizio di porting policy è obbligatorio ed il relativo costo è da intendersi compreso nei corrispettivi previsti per i prodotti offerti.
Tale servizio riguarda il caso in cui il prodotto sia acquistato in sostituzione di un prodotto già presente presso l’Amministrazione. In tal caso, in particolare, il Fornitore dovrà garantire l’analisi delle impostazioni/policy/configurazioni per l’eventuale migrazione, relativamente alle attività funzionali per la messa in opera del nuovo prodotto. Non sono ricomprese nel servizio le configurazioni avanzate del prodotto stesso, che afferiranno invece al servizio di supporto specialistico.
Le attività, i deliverable e le relative tempistiche dovranno essere indicate nel Piano di lavoro generale.

2.2.3 Servizio di monitoraggio e aggiornamento software/firmware (incluso nella fornitura)

Il servizio di monitoraggio e aggiornamento software/firmware è obbligatorio ed il relativo costo è da intendersi compreso nei corrispettivi previsti per i prodotti offerti.

~~Gli aggiornamenti di firmware/software dovranno essere garantiti dal Fornitore all’Amministrazione per la durata di 36 mesi, decorrenti dalla data di accettazione della fornitura del rispettivo prodotto. Si intendono incluse nel servizio tutte le eventuali nuove minor release e le licenze/subscription che garantiscano il corretto funzionamento del prodotto per 36 mesi dalla “Data di accettazione” della fornitura del rispettivo prodotto.~~

Per i prodotti offerti in formato Appliance Fisica, gli aggiornamenti firmware/software dovranno essere garantiti per 36 mesi decorrenti dalla Data di Accettazione della relativa fornitura. Si intendono

incluse nel servizio tutte le eventuali nuove minor release e le licenze/subscription necessarie a garantire il corretto funzionamento del prodotto per il medesimo periodo.

Per i prodotti offerti negli ulteriori formati tecnologici, gli aggiornamenti firmware/software dovranno essere garantiti per l'intera durata della relativa fornitura, fino a un massimo di 36 mesi, decorrenti dalla Data di Accettazione della fornitura del rispettivo prodotto.

Si intendono incluse nel servizio tutte le eventuali nuove minor release e le licenze/subscription necessarie a garantire il corretto funzionamento del prodotto per l'intera durata della relativa fornitura.

Il Fornitore è tenuto a monitorare costantemente il rilascio, da parte del Vendor, degli aggiornamenti software/firmware e patch di sicurezza, relativi ai prodotti forniti e a comunicarne tempestivamente la disponibilità all'Amministrazione, entro le tempistiche previste dall'indicatore di qualità IQ13 di cui al successivo paragrafo 3.13.
La comunicazione dovrà riportare almeno:

- il prodotto e le versioni interessate;
- la data di pubblicazione dell'aggiornamento o della patch da parte del Vendor;
- la tipologia e la descrizione sintetica dell'aggiornamento;
- l'eventuale identificativo CVE;
- il livello di criticità secondo la classificazione CVSS, ove applicabile;
- l'eventuale sfruttamento attivo della vulnerabilità;
- la disponibilità della correzione rilasciata dal Vendor;
- le eventuali misure temporanee di mitigazione;
- gli eventuali impatti, prerequisiti, dipendenze e indisponibilità connessi all'applicazione dell'aggiornamento;
- le indicazioni del Vendor relative alle modalità e alle tempistiche di applicazione.

Ai fini della classificazione delle vulnerabilità, il Fornitore tiene conto delle informazioni pubblicate nei bollettini ufficiali del Vendor, con particolare riferimento all'identificativo CVE, al punteggio CVSS, alle versioni interessate e alla disponibilità di correzioni o misure di mitigazione. Il Fornitore tiene altresì conto, ove disponibili, degli alert e dei bollettini pubblicati dall'ACN/CSIRT Italia, con particolare riferimento all'impatto sistemico, all'eventuale sfruttamento attivo della vulnerabilità e alle azioni di mitigazione indicate. In caso di aggiornamento delle informazioni pubblicate, si tiene conto dell'ultima versione disponibile.

A seguito della comunicazione del Fornitore, l'Amministrazione potrà:

- richiedere al Fornitore di provvedere all'installazione o all'applicazione dell'aggiornamento software/firmware, della patch di sicurezza o della misura temporanea di mitigazione;
- provvedere autonomamente, oppure tramite un soggetto terzo dalla stessa incaricato, alla relativa installazione o applicazione;

- programmare l'installazione o l'applicazione, tenuto conto delle proprie esigenze operative e di continuità del servizio, sulla base di un piano di lavoro concordato.

Qualora l'Amministrazione richieda al Fornitore di eseguire l'intervento, le modalità e le tempistiche di installazione o applicazione degli aggiornamenti software/firmware e delle patch di sicurezza, sia ordinari sia connessi alla correzione di vulnerabilità, dovranno essere definite nel Piano di Lavoro Generale, tenendo conto delle indicazioni del Vendor, delle caratteristiche della soluzione e del relativo modello di erogazione, del contesto tecnologico e delle esigenze di continuità operativa dell'Amministrazione. Nel caso di aggiornamenti connessi alla correzione di vulnerabilità, dovranno essere considerati anche il relativo livello di criticità e l'eventuale sfruttamento attivo.

Gli aggiornamenti e le patch di sicurezza dovranno essere installati o applicati nel rispetto delle procedure, delle modalità operative, delle finestre temporali e delle modalità di accesso concordate con l'Amministrazione.

Qualora l'Amministrazione decida di provvedere autonomamente oppure tramite un soggetto terzo, il Fornitore dovrà rendere disponibili, senza ulteriori oneri, l'aggiornamento, la patch, le relative note tecniche e ogni altra informazione resa disponibile dal Vendor e necessaria alla corretta esecuzione dell'intervento. In tale ipotesi, l'attività di installazione o applicazione non è posta a carico del Fornitore.

Restano escluse dal servizio obbligatorio di aggiornamento software/firmware le ulteriori attività di analisi tecnica, hardening, modifica delle configurazioni, integrazione con altri sistemi e supporto operativo, che sono svolte nell'ambito dei servizi opzionali di manutenzione o di supporto specialistico, qualora acquistati dall'Amministrazione e secondo il rispettivo perimetro contrattuale.

Il rispetto delle tempistiche relative all'installazione o all'applicazione degli aggiornamenti e delle patch di sicurezza è verificato mediante l'indicatore di qualità IQ14 di cui al successivo paragrafo 3.14.

2.2.4 Servizio di manutenzione (opzionale)

Il servizio di manutenzione è opzionale (sebbene oggetto di quotazione) e quindi dovrà essere prestato, a pagamento, dal Fornitore soltanto se espressamente richiesto dall'Amministrazione nell'ambito del Piano dei Fabbisogni.
Il servizio di manutenzione si applica alle componenti di fornitura per le quali l'Amministrazione e/o il Fornitore hanno responsabilità operative dirette. Per le soluzioni erogate in formato Cloud/SaaS, restano fermi i livelli di servizio e le condizioni di disponibilità del servizio.

Le attività, i deliverable e le relative tempistiche dovranno essere indicate nel Piano di lavoro generale.

Il servizio di manutenzione deve essere prestato dal Fornitore nel rispetto degli SLA di seguito descritti, anche con interventi da effettuarsi presso i siti dell'Amministrazione.

La manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti ed il ripristino delle funzionalità, anche attraverso attività di supporto on-site.

Sarà facoltà dell'Amministrazione richiedere a pagamento il servizio manutenzione in base al profilo di qualità richiesto per i servizi erogati, *Low Profile* (*Business Day*) o *High Profile* (*H24*).

LOW PROFILE = LP (BUSINESS DAY)	HIGH PROFILE = HP (H24)
Lun-Ven 9.00 - 18.00	H24, 7 giorni su 7

Tabella 22 - Finestra di erogazione dei servizi

Per l'esecuzione delle attività richieste nei tempi previsti, l'Amministrazione dovrà consentire l'accesso alle aree interessate dagli interventi, ove necessario.
Relativamente ai servizi di manutenzione, i guasti segnalati al Service Desk fornito dall'Aggiudicatario saranno codificati secondo una classe di severità (**Severity Code**), in base alla gravità del problema riscontrato. L'assegnazione dello specifico Severity Code dovrà essere repentinamente segnalata e formalizzata tramite e-mail. Sulla base del Severity Code assegnato l'operatore del servizio di assistenza da remoto dovrà fornire una stima dei tempi di ripristino e delle modalità di intervento nel rispetto dei parametri di SLA nel seguito definiti, eventualmente avvalendosi della possibilità di effettuare una prima diagnosi da remoto.

I Severity Code sono identificati nella Tabella seguente:

SEVERITY CODE	
SEVERITY CODE 1	Guasto Bloccante: le funzionalità di base e/o maggiormente rilevanti non sono più operative o fortemente compromesse.
SEVERITY CODE 2	Disservizio: le funzionalità di base sono operative ma il loro utilizzo non è soddisfacente.

Tabella 23 – Classificazione dei Severity Code

Le tempistiche di risposta, intervento e ripristino sono indicate al successivo capitolo 3, in corrispondenza degli specifici indicatori di qualità: i termini ivi indicati sono eventualmente migliorati in offerta tecnica.
Pertanto, per il monitoraggio delle attività ricomprese nel servizio di manutenzione, l'Amministrazione terrà conto di quanto indicato negli indicatori di qualità specifici.

Resta inteso che, indipendentemente dalla finestra di erogazione associata al profilo selezionato, qualora gli interventi di manutenzione dovessero comportare una completa interruzione dell'attività lavorativa dei dipendenti dell'Amministrazione, gli interventi stessi dovranno essere effettuati in orario non coincidente con il periodo di operatività dell'Amministrazione. Tutti gli interventi di manutenzione dovranno in ogni caso essere concordati preventivamente con l'Amministrazione.

Il Fornitore sarà tenuto ad offrire il servizio di manutenzione per annualità, quindi per 12 mesi, 24 mesi o 36 mesi.
L'Amministrazione pertanto potrà richiedere, in sede di Piano dei Fabbisogni, il servizio di manutenzione, indicandone la durata (che potrà essere di 12, di 24 o di 36 mesi) e la decorrenza, fermo restando che il servizio non potrà essere attivato prima della "data di accettazione" della fornitura relativa al rispettivo prodotto e non potrà avere una durata superiore rispetto alla scadenza del contratto (anche eventualmente prorogata nei casi previsti dall'Accordo Quadro e comunque dalla normativa vigente).

Nell'esecuzione delle attività richieste, il Fornitore avrà la facoltà, previo accordo con l'Amministrazione, di predisporre un accesso remoto sicuro a supporto delle stesse, ad esempio per effettuare diagnosi, attraverso i propri sistemi di gestione e management, su problematiche e malfunzionamenti segnalati dall'Amministrazione.
L'accesso remoto dovrà essere effettuato mediante account VPN personali opportunamente configurati e abilitati, con tracciatura degli accessi ai fini di eventuali audit e limitazione degli stessi al tempo strettamente necessario all'esecuzione delle attività, anche mediante utenze temporanee create all'occorrenza.
In caso di accesso mediante utenze con privilegi amministrativi, il Fornitore dovrà utilizzare, su richiesta dell'Amministrazione, gli strumenti messi a disposizione dalla stessa per la gestione e la protezione degli accessi, comprese eventuali soluzioni PAM e meccanismi di autenticazione a più fattori.
Le modalità operative relative agli accessi da remoto dovranno essere indicate nel Piano di Lavoro Generale e concordate con l'Amministrazione Contraente in sede di presa in carico. Tali modalità dovranno garantire il rispetto delle disposizioni e delle prassi in materia di sicurezza e protezione dei dati personali, nonché delle policy di sicurezza definite dall'Amministrazione.

Le attività di manutenzione potranno essere richieste dalle Amministrazioni Contraenti sui soli elementi di fornitura acquistati nell'ambito del Lotto di riferimento.

Le attività di manutenzione possono riassumersi in:

- ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code;
- risoluzione del problema tramite supporto telefonico all'utente (ove possibile) e/o eventuale intervento/i remoto/i;
- risoluzione della causa del guasto tramite, ove necessario:
    - intervento presso la sede/luogo interessato;
    - ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati;
    - verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto/malfunzionamento.

Ogni intervento di manutenzione dovrà prevedere la redazione del relativo *Verbale di Intervento* e l'eventuale aggiornamento della documentazione di progetto.

Gli interventi dovranno concludersi con l'attività di verifica del corretto funzionamento dei prodotti, delle apparecchiature sostituite o riparate (ove necessario e/o pertinente) e del sistema nella sua globalità; tale verifica sarà a cura del Fornitore, ma è lasciata libertà all'Amministrazione di coinvolgere proprio personale e/o personale di terzi. L'Aggiudicatario è tenuto al rispetto delle modalità operative richieste dall'Amministrazione.

Tutte le attività previste (interventi del Fornitore presso l'Amministrazione, rimozione degli elementi, riparazione degli elementi guasti, successiva installazione, nuova installazione software/appliance virtuali) sono da intendersi **incluse nel costo del servizio**.

Il servizio dovrà inoltre comprendere:

- **l'attivazione, sui prodotti manutenuti, di tutte le eventuali *Major release* successive a quella installata sui prodotti acquisiti emesse dal produttore nel periodo di validità del servizio;**
- **le attività di hardening in caso di cambiamenti (come aggiornamenti software/patch, modifiche alle configurazioni, cambio sistemi con cui il prodotto si interfaccia/integra, etc) e, ove non intervengano, una rivalutazione almeno annuale.**

Si precisa infine che, in caso di malfunzionamenti inerenti la componente software/firmware, il Fornitore dovrà farsi carico di informare tempestivamente le Amministrazioni che hanno acquisito i medesimi prodotti provvedendo a tutte le attività volte all'aggiornamento della componente software/firmware soggetta al malfunzionamento. Tale attività dovrà essere svolta sia nel caso in cui il malfunzionamento sia identificato proattivamente dal Fornitore o dal produttore, sia nel caso esso sia identificato da un'Amministrazione Contraente. Dovrà essere prestata particolare attenzione a quanto attiene **bug o problematiche che possano compromettere le funzionalità di sicurezza cui i prodotti acquistati sono destinati**, rendendo di fatto, sia loro sia i sistemi da loro protetti, **vulnerabili a *exploit***. In tale eventualità il Fornitore dovrà, oltre ad attivarsi tempestivamente per procedere alla risoluzione della problematica e all'aggiornamento dei sistemi, fornire eventuali *work-around* (documentati e inviati all'Amministrazione) che consentano di eliminare o quanto meno attenuare il rischio di sfruttamento delle falle identificate da parte di soggetti non autorizzati.

Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento è: somma delle quantità ordinate moltiplicate per la **percentuale del valore di fornitura rispetto al profilo di manutenzione richiesto**.
La modalità di remunerazione di tutti i servizi è: **canone trimestrale**.

In fase di offerta economica al concorrente sarà richiesto di esprimere due valori percentuali in base al profilo di qualità richiesto per i servizi erogati, *Low Profile* (*Business Day*) o *High Profile* (*H24*). Ogni valore espresso rappresenta la percentuale del prezzo di fornitura degli elementi offerti in Accordo Quadro relativa al canone di manutenzione annuale (ad esempio: se il prezzo dell'elemento di fornitura "X" offerto dal concorrente è pari a 10€ e la percentuale relativa alla manutenzione per il profilo *Low Profile* offerta dal concorrente è pari al 10% il corrispondente canone annuale della manutenzione con profilo *Low Profile* dell'elemento di fornitura "X" è pari a 10€ x 10% = 1€).

2.2.5 Servizio di formazione e affiancamento (opzionale)

Il servizio di formazione e affiancamento è opzionale (sebbene oggetto di quotazione), quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario solo se espressamente richiesto dall'Amministrazione.

Il servizio consente la fruizione di sessioni formative impartite presso le sedi dell'Amministrazione che permettano di istruire i discenti sulle specifiche tecnologie acquistate nell'Accordo Quadro, e deve avere l'obiettivo di:

- istruire i discenti sulle principali minacce che i prodotti acquistati si prefiggono di contrastare;
- descrivere gli apparati installati 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 componenti installate in maniera autonoma ed ottimale;
- descrivere le eventuali attività di integrazione effettuate con altri prodotti acquistati o con prodotti già presenti 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 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 2.2.6.3 per le figure di Senior 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 che attengono al solo supporto specialistico. 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 4. 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.

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 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 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 effettiva, il programma effettivamente seguito ed eventuali criticità emerse.

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

Il servizio potrà essere acquisito solo contestualmente ai prodotti. In fase di offerta è richiesto al Concorrente di esprimere un prezzo per modulo formativo come in precedenza descritto.

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.

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**.

2.2.6 Servizio di supporto specialistico (opzionale)

2.2.6.1 Descrizione del servizio

Il servizio di supporto specialistico è opzionale (sebbene oggetto di quotazione), quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario soltanto se espressamente richiesto dall'Amministrazione nel Piano dei Fabbisogni.

Tale servizio consente alle Amministrazioni Contraenti di richiedere apposito supporto, erogato da personale specializzato, rispetto alle seguenti (tassative) attività inerenti la fornitura specifica acquistata nell'ambito dell'Accordo Quadro:

a) la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso;
b) l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi acquistati dall'Amministrazione;
c) il supporto al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Amministrazione, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa.

L'erogazione del servizio dovrà essere garantita dalla *Data di accettazione* della fornitura relativa al **primo** prodotto collaudato e dovrà essere garantito fino alla scadenza del Contratto Esecutivo (anche eventualmente prorogata nei casi previsti dall'Accordo Quadro e comunque dalla normativa vigente). La descrizione delle attività previste e il relativo effort saranno riportate nel Piano di Lavoro Generale (in coerenza con quanto riportato nel Piano dei Fabbisogni e nel Piano Operativo).

L'Amministrazione potrà richiedere al Fornitore che il servizio sia erogato secondo le seguenti modalità:

i. in fase iniziale - lett. a) del precedente elenco;
ii. in modalità "*spot*" - lett. b) e lett c) (limitatamente alla modalità "a chiamata") del precedente elenco;
iii. con periodicità definita - lett. c) (limitatamente alla modalità "presidio").

Si precisa che anche in caso di richiesta in modalità "spot" il servizio dovrà essere richiesto dall'Amministrazione nel Piano dei Fabbisogni, con indicazione del numero massimo di giorni persona stimato.

In particolare, in caso di necessità di attivazione della modalità "*spot*" in corso di vigenza di contratto esecutivo, l'Amministrazione invierà una *Richiesta di attivazione del servizio di supporto* all'Aggiudicatario tramite uno dei canali messi a disposizione con la descrizione dell'attività richiesta, dichiarando le tempistiche richieste per l'erogazione del servizio. L'Amministrazione potrà inoltre preventivamente contattare l'Aggiudicatario per meglio delimitare il perimetro dell'intervento richiesto ed il relativo effort. Entro **2 giorni lavorativi** dalla ricezione della *Richiesta di attivazione del servizio di supporto*, l'Aggiudicatario sarà tenuto a inviare una *Lettera di presa in carico del servizio di supporto* nella quale dovrà indicare il numero identificativo della lavorazione, l'effort e le tempistiche richieste dall'Amministrazione nella richiesta effettuata o successivamente concordate con l'Amministrazione stessa, inclusa la data di completamento dell'intervento. Il mancato rispetto dei tempi concordati è oggetto di penale. In particolare, per la modalità "spot", la data di completamento dell'intervento non potrà superare la data concordata con l'Amministrazione. Al termine delle attività l'Aggiudicatario dovrà fornire un documento di *Rapporto di Fine Intervento* che specifichi la data di avvio dell'intervento, le attività eseguite, la durata dell'intervento e la data di completamento.

L'Aggiudicatario dovrà:

- in caso di servizio richiesto in fase iniziale o con periodicità definita - precedenti punti i) e iii): presentare all'Amministrazione Contraente, entro le tempistiche indicate al paragrafo 3.3.4 del Capitolato Tecnico Generale, i CV delle risorse proposte per l'erogazione del servizio in cui dovranno essere anche inserite copie delle certificazioni possedute dalle risorse, in accordo con i requisiti minimi o i migliorativi eventualmente offerti;
- in caso di servizio richiesto in modalità "spot" – precedente punto ii): presentare all'Amministrazione Contraente, entro 5 giorni solari dalla data di invio della *Lettera di presa in carico del servizio di supporto*, i CV delle risorse proposte per l'erogazione del servizio in cui dovranno essere anche inserite copie delle certificazioni possedute dalle risorse, in accordo con i requisiti minimi o i migliorativi eventualmente offerti.

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. 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. 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.

I curriculum vitae delle figure professionali da impiegare dovranno essere resi disponibili alle Amministrazioni rispettando lo schema indicato al capitolo 4. 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.

2.2.6.2 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~~ 8.00 o la domenica o nei giorni festivi (fascia straordinaria).

In sede di Piano dei fabbisogni, l'Amministrazione indicherà le attività, i deliverables e le risorse necessarie, indicando quindi il mix necessario per le attività richieste, in un'ottica di coerenza e proporzionalità, come meglio indicato al successivo paragrafo.

2.2.6.3 Risorse da impiegare nell'esecuzione del servizio di supporto specialistico

Con riferimento ai servizi di supporto specialistico dei Lotti 2, 3 e 4, 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 e seguendo l'evoluzione del prodotto/tecnologia a cui si riferiscono;
- una certificazione può, nel corso del singolo Contratto Esecutivo, nei casi espressamente autorizzati dall'Amministrazione, essere sostituita da comprovate esperienze di almeno 4 anni sul prodotto/tecnologia oggetto della certificazione (resta fermo in ogni caso il possesso delle certificazioni espressamente offerte in AQ dal fornitore).

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 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 24. 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.

FIGURA PROFESSIONALE	SECURITY PRINCIPAL
TITOLO DI STUDIO	Laurea magistrale/specialistica in discipline scientifiche
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 10 (dieci) anni nel settore ICT, di cui almeno 5 (cinque) anni di provata esperienza nella specifica funzione
CERTIFICAZIONI	Possesso di almeno una certificazione in ambito program e project management, quali ad esempio: Prince2 Practitioner, PgMP, PMP, UNI 11648
COMPETENZE ED ESPERIENZE RICHIESTE	Conoscenza delle metodologie di program e project management
	Conoscenza approfondita della normativa nazionale ed europea in ambito ICT Security e Privacy
	Conoscenza approfondita dei processi di security governance e security management
	Conoscenza approfondita delle metodologie e dei processi in ambito ict security e privacy quali: risk management, business continuity, vulnerability assessment & penetration test, incident handling ed escalation per la gestione degli incidenti di sicurezza informatica, classificazione e gestione delle informazioni, gestione delle utenze, gestione degli end point, security audit, etc
	Conoscenza dei processi e delle procedure operative ICT
	Conoscenza ed esperienza sulle tecnologie principali per la sicurezza ict (si cita a titolo esemplificativo e non esaustivo NGFW, WAAP, IAM; DLP, SIEM, SOAR, etc)
	Conoscenza dei principali standard e framework di sicurezza e privacy quali: ISO /IEC 27001; ISO/IEC: 27017; ISO/IEC 27018; ISO 22301; ITIL, COBIT; CMMI; CISM; CISA; NIST, etc
	Esperienza di Project Management in progetti analoghi e in contesti di diversa complessità
	Esperienza consolidata nella gestione di progetti/programmi in ambito ICT Security e Privacy
	Esperienza consolidata nel disegno e nella valutazione dei sistemi di gestione della sicurezza e della privacy delle informazioni, nonché nella gestione della continuità operativa

FIGURA PROFESSIONALE	SECURITY ARCHITECT
TITOLO DI STUDIO	Laurea magistrale/specialistica in discipline scientifiche
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 8 (otto) anni nel settore ICT, di cui almeno 4 (quattro) anni di provata esperienza nella specifica funzione

FIGURA PROFESSIONALE	SECURITY ARCHITECT
CERTIFICAZIONI	Possesso delle massime certificazioni di prodotto tecnico/professionali, ottenibili dai vendor delle soluzioni offerte.
COMPETENZE ED ESPERIENZE RICHIESTE	Capacità di comprendere l'infrastruttura sotto analisi e le relazioni tra i differenti sistemi e componenti infrastrutturali
	Conoscenza di norme e standard adottati per l'hardening ed il patching dei sistemi operativi, servizi e applicazioni
	Conoscenza della normativa nazionale ed europea in ambito ICT Security e Privacy
	Conoscenza approfondita delle problematiche di sicurezza delle infrastrutture ICT e IT/OT
	Conoscenza delle metodologie e degli strumenti operativi richiesti per verificare l'efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture ICT
	Conoscenza delle tecnologie principali per la sicurezza ICT, soprattutto in ambito sicurezza cloud e prodotti SaaS, minacce di nuova generazione e modalità di contenimento, utilizzo ml/ai nelle soluzioni adottate, ecc.
	Conoscenza dei sistemi di correlazione eventi, progettazione regole di correlazione e tuning sistemi di analisi eventi con esperienza di integrazione in contesti analoghi
	Buona conoscenza dei principi e dei sistemi di autenticazione, specialmente sistemi di Identity & Access Management, di Data Classification, di gestione certificati, con esperienza di integrazione su ambienti analoghi
	Conoscenza delle tecnologie in uso nel contesto di riferimento dei Lotti di fornitura dei prodotti, con esperienza nella configurazione e nell'inserimento in rete delle stesse, in funzione delle minacce riscontrate
	Conoscenza dei principali standard e framework di sicurezza e privacy quali: ISO /IEC 27001, ISO/IEC: 27017, ISO/IEC 27018, ISO 22301; CISSP, CCSP, CSSLP, CISM, NIST, OWASP, SANS/SEC-540, etc
	Esperienza nell'analisi e nella valutazione delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (reti TCP/IP, NGFW, SIEM, DLP, soluzioni anti-malware, WAAP, soluzione cloud oriented per la sicurezza, ecc.)
	Consolidata esperienza nella progettazione della sicurezza ICT maturata in contesti analoghi

FIGURA PROFESSIONALE	SECURITY ARCHITECT
	Esperienza nell'analisi di un'infrastruttura ICT complessa volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza
	Esperienza nella verifica dell'efficacia delle misure tecniche ed organizzative preposte alla sicurezza di un'infrastruttura ICT complessa
	Esperienza nell'identificazione di soluzioni tecnologiche ed organizzative da porre in essere per ottimizzare e migliorare le configurazioni e le politiche e per traguardare la piena adozione delle contromisure previste

FIGURA PROFESSIONALE	SENIOR SECURITY ANALYST
TITOLO DI STUDIO	Laurea magistrale/specialistica in discipline scientifiche
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 6 (sei) anni nel settore ICT, di cui almeno 4 (quattro) anni di provata esperienza nella specifica funzione
CERTIFICAZIONI	Nessuna Certificazione
COMPETENZE ED ESPERIENZE RICHIESTE	Capacità di coordinamento delle risorse Junior
	Conoscenza dei processi e delle procedure operative ICT
	Conoscenza approfondita dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica
	Conoscenza approfondita dei processi di analisi forense, acquisizione degli elementi probatori e conservazione degli stessi
	Conoscenza approfondita dei sistemi di rilevazione e analisi degli allarmi
	Conoscenza dei processi di reverse engineering dei malware ed esperienza consolidata nella analisi forense di malware mediante strumenti di analisi e attività di reverse
	Conoscenza approfondita dei protocolli di rete e della tipologia di traffico all'interno di un contesto complesso con esperienza consolidata nell'analisi forense del traffico di rete e nell'identificazione di anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza
	Conoscenza di "EC-Council CSA (Certified SOC Analyst)" e/o "CompTIA CySA+ (Cyber Security Analyst)" e/o "GIAC Certied Intrusion Analyst"
	Esperienza consolidata nella definizione di configurazioni e analisi di sicurezza
	Esperienza nella definizione di regole di correlazione e nel tuning delle stesse

FIGURA PROFESSIONALE	SECURITY SPECIALIST
TITOLO DI STUDIO	Laurea magistrale/specialistica in discipline scientifiche
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 5 (cinque) anni nel settore ICT, di cui almeno 2 (due) anni di provata esperienza nella specifica funzione
CERTIFICAZIONI	Possesso delle certificazioni di prodotto tecnico/professionali superiori al livello base, ottenibili dal vendor delle soluzioni offerte.
COMPETENZE ED ESPERIENZE RICHIESTE	Capacità di comprendere il contesto tecnologico in analisi e di identificare le minacce cyber
	Capacità di identificare ed implementare le adeguate misure difensive
	Capacità di eseguire risk assessment
	Capacità di effettuare attività di Vulnerability Assessment e Penetration Test
	Conoscenza delle problematiche di sicurezza delle infrastrutture ICT
	Conoscenza delle tecnologie principali per la sicurezza ICT, compreso l'ambito sicurezza cloud, sicurezza minacce di nuova generazione, modalità di contenimento, ML/AI, ecc.
	Ottima conoscenza sistemi di correlazione eventi, progettazione regole di correlazione e tuning sistemi di analisi eventi con esperienza di integrazione in contesti analoghi
	Buona conoscenza sistemi di autenticazione, specialmente sistemi di Identity & Access Management con esperienza di integrazione su ambienti analoghi
	Conoscenza delle tecnologie in uso nel contesto di riferimento, con esperienza nella configurazione e nell'inserimento in rete delle stesse, in funzione delle minacce riscontrate
	Conoscenza di alcuni principali standard e framework di sicurezza e privacy quali: ISO/IEC 27001; CISM; CCSK; CISSP; CompTIA Security+; CEH; PSI-DSS; Nist, etcq
	Esperienza nella verifica dell'efficacia delle misure tecniche ed organizzative preposte alla sicurezza di un'infrastruttura ICT complessa
	Esperienza nell'analisi, nella valutazione e nell'implementazione delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (reti TCP/IP, NGFW, SIEM, DLP, soluzioni anti-malware, WAAP, soluzione cloud oriented per la sicurezza, IAM, ecc.)

FIGURA PROFESSIONALE	SECURITY SPECIALIST
	Esperienza nella progettazione e gestione della sicurezza ICT e delle relative soluzioni maturata in contesti analoghi
	Esperienza nell'analisi tecnica di incidenti e nella modalità di intervento
	Esperienza nelle attività di Hardening e Patching

FIGURA PROFESSIONALE	JUNIOR SECURITY CONSULTANT
TITOLO DI STUDIO	Laurea triennale in discipline scientifiche
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 3 (tre) anni nel settore ICT, di cui almeno 2 (due) anni di provata esperienza nella specifica funzione
CERTIFICAZIONI	Nessuna Certificazione
COMPETENZE ED ESPERIENZE RICHIESTE	Conoscenza dei processi e delle procedure operative ICT
	Conoscenza dei processi di: risk management, vulnerability assessment & penetration test, Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica, classificazione e gestione delle informazioni, gestione delle utenze, gestione degli end point, Hardening e Patching, etc
	Conoscenza dei sistemi di rilevazione e analisi degli allarmi
	Conoscenza della modalità di intervento sulle postazioni client e sui server in caso di diffusione di malware di nuova generazione
	Conoscenza delle principali tecnologie in ambito ICT Security (si cita a titolo esemplificativo e non esaustivo NGFW, WAAP, IAM; DLP, SIEM, SOAR, etc)
	Conoscenza dei protocolli di rete e della tipologia di traffico all'interno di un contesto ICT
	Conoscenza di alcuni principali standard e framework di sicurezza e privacy quali: ISO/IEC 27001; ISO/IEC:27017; ISO/IEC 27005; ISO/IEC 27018; ISO 22301; ITIL; COBIT; Nist; etc
	Conoscenza della normativa nazionale ed europea in ambito ICT Security e Privacy
	Conoscenza delle diverse tipologie di attacco informatico, delle tecniche di penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente
	Esperienza nell'analisi tecnica di incidenti
	Esperienza di affiancamento e supporto nelle attività di Vulnerability Assessment e Penetration Test
	Esperienza in progetti in ambito security e privacy

3 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 conforme, fatto salvo il risarcimento del maggior danno.

3.1 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;
- Piano di lavoro Generale;
- CV delle risorse e dei responsabili tecnici con le relative certificazioni;
- Deliverable di fornitura;
- Tempistiche di risoluzioni problemi in Collaudo, di cui al corrispondente paragrafo.

ASPETTO DA VALUTARE	RISPETTO DI UNA SCADENZA CONTRATTUALE		
Unità di misura	Giorni lavorativi	**Fonte dati**	Comunicazioni Note Amministrazione Verbali di riunioni
Periodo di riferimento	Durata della fornitura Periodi di verifica di conformità/Collaudo	**Frequenza di misurazione**	Trimestrale 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	$IQ01 = 0$		
Azioni contrattuali	Il mancato rispetto del valore di soglia comporterà per ogni giorno lavorativo di ritardo rispetto al valore soglia 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 per ogni giorno (solare o lavorativo a seconda di quanto indicato nel corrispondente paragrafo di riferimento) di ritardo rispetto al valore soglia 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

3.2 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 DA VALUTARE	**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**	Trimestrale
Dati da rilevare	*N_ris_inad* = Numero di risorse sostituite su richiesta dell'Amministrazione perché non rispondenti ai requisiti		
Regole di campionamento	Nessuna		
Formula	*IQ02 = N_ris_inad*		
Regole di arrotondamento	Nessuna		
Valore di soglia	*IQ02 = 1*		
Azioni contrattuali	Il mancato rispetto del valore di soglia comporterà per ogni risorsa eccedente il valore di soglia nel periodo di riferimento l'applicazione della penale **"Risorse Impiegate nell'erogazione del servizio non rispondenti ai requisiti"**, pari **allo 0,6‰** (zerovirgolasei per mille), dell'importo del Contratto esecutivo.		
Applicazione	Amministrazione Contraente		
Eccezioni	Nessuna		

3.3 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, che 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**	Trimestrale
Dati da rilevare	*N_ris_inad* = Numero di risorse sostituite per inadeguatezza su richiesta di Consip o dell'Amministrazione		
Regole di campionamento	Nessuna		
Formula	*IQ03 = N_ris_inad*		
Regole di arrotondamento	Nessuna		
Valore di soglia	*IQ03 = 0*		
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà per la sostituzione del RUAC dell'Accordo Quadro rispetto al valore soglia 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 per ogni risorsa di Responsabile tecnico del Fornitore sostituito rispetto al valore soglia l'applicazione della penale "**Adeguatezza del personale impiegato nei ruoli contrattuali** –" pari allo **0,6‰** (zerovirgolasei per mille) dell'importo del Contratto esecutivo.		
Applicazione	Consip e Amministrazione Contraente		
Eccezioni	Nessuna		

3.4 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 DA VALUTARE	**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 Verbali
Periodo di riferimento	Durata della fornitura	**Frequenza di misurazione**	Trimestrale
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 (trimestrale)		
Regole di campionamento	Nessuna		
Formula	$IQ04 = \sum(data_eff - data_prev)$		
Regole di arrotondamento	Nessuna		
Valore di soglia	$IQ04 = 5$		
Azioni contrattuali	Il mancato rispetto del valore di soglia comporterà 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 l'applicazione della penale **"Adeguatezza dei tempi di sostituzione delle figure professionali proposte per la erogazione dei servizi"**, pari **allo 0,6‰** (zerovirgolasei per mille), dell'importo del Contratto esecutivo.		
Applicazione	Amministrazione Contraente		
Eccezioni	Nessuna		

3.5 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 DA VALUTARE	NUMERO DI RISORSE SOSTITUITE SU INIZIATIVA DEL FORNITORE		
Unità di misura	Risorse	**Fonte dati**	E-mail lettere verbali
Periodo di riferimento	Durata della fornitura	**Frequenza di misurazione**	Trimestrale
Dati da rilevare	Numero risorse sostituite su iniziativa del Fornitore *(Nrisorse_sostituite)*		
Regole di campionamento	Nessuna		
Formula	*IQ05 = Nrisorse_sostituite*		
Regole di arrotondamento	Nessuna		
Valore di soglia	*IQ05 = 1*		
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà per ogni risorsa aggiuntiva rispetto al valore soglia l'applicazione della penale "**Turnover del personale impiegato nella fornitura**" pari a **€ 1.000,00 (mille/00)**.		
Applicazione	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 purché sia rispettata almeno una delle seguenti condizioni:
	  – ciascuna sostituzione sia effettuata nel rispetto dei termini del preavviso previsti dal contratto di lavoro applicato;
	  – ciascuna sostituzione deve essere preventivamente approvata dall'Amministrazione;		

	– ciascuna dimissione sia opportunamente documentata.

3.6 IQ06 – Impegni assunti in offerta tecnica

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

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

L'indicatore di qualità è definito come la percentuale, consolidata su base trimestrale, 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.

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	Durata della fornitura Periodi di verifiche di conformità/Collaudo	**Frequenza di misurazione**	Trimestrale
Dati da rilevare	-Data e Ora (hh/mm/ss/dd) di avvio dell'interazione (*Data_avvio*) -Data e Ora (hh/mm/ss/dd) della effettiva risposta (*Data_risp*) -Numero totale interazioni pervenute nel periodo di riferimento (*Num_tot*)		
Regole di campionamento	Nessuna		
Formula	*IQ07* = *Num_interazioni* (*T_risp* <= ***T_ottimale***) / *Num_tot* Dove: *T_risp* = *Data_risp* – *Data_avvio* *T_ottimale* = 120 secondi		
Regole di arrotondamento	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 per ogni punto percentuale in diminuzione rispetto al valore soglia nel periodo di riferimento, l'applicazione della penale **"Tempestività di risposta"** pari a € 300,00 (trecento/00).		
Applicazione	Amministrazione Contraente		
Eccezioni	Nessuna		

3.8 IQ08 – Percentuale di chiamate in ingresso perse per il servizio di Service Desk

L'indicatore di qualità identifica la percentuale di chiamate in ingresso perse per Contratto Esecutivo.
Si definisce chiamata persa quella telefonata:

- a cui segue il segnale di occupato;
- che viene messa in diretto contatto con la segreteria telefonica (soluzione ammessa solo per chiamate fuori orario di servizio con operatore).

Detto valore viene valutato considerando il numero delle chiamate consolidato su base mensile.

ASPETTO DA VALUTARE	CHIAMATE IN INGRESSO PERSE PER IL SERVIZIO DI SERVICE DESK		
Unità di misura	Percentuale	**Fonte dati**	Comunicazioni Contratto Esecutivo Piano di Lavoro Strumenti di Tracciatura
Periodo di riferimento	Durata della fornitura Periodi di verifiche di conformità/Collaudo	**Frequenza di misurazione**	~~Trimestrale~~ Mensile
Dati da rilevare	- Numero di Chiamate cui segue il segnale di occupato (NC_Occ) - Numero di Chiamate inoltrate automaticamente alla segreteria telefonica (NC_Segr) Numero totale di Chiamate realizzate (NC_Tot)		
Regole di campionamento	Vanno considerate tutte le richieste pervenute nel periodo di riferimento		
Formula	*IQ08 = NC_Inevase / NC_Tot* Dove: *NC_Inevase = NC_Occ + NC_Segr*		
Regole di arrotondamento	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	*IQ08 = 4%*		

Azioni contrattuali	Il mancato rispetto del valore soglia comporterà per ogni punto percentuale in aumento rispetto al numero dei campioni di misura del parametro nel periodo di riferimento, l'applicazione della penale **"Percentuale di chiamate in ingresso perse"** pari a **€ 1.000,00** (mille/00).
Applicazione	Amministrazione Contraente
Eccezioni	Nessuna

3.9 IQ09 – Tempestività di risposta al disservizio

È definito, nell'ambito del servizio di manutenzione, come lo scostamento tra il tempo misurato ed i valori target (in base al profilo) in relazione alla segnalazione del disservizio da parte dell'Amministrazione Contraente al servizio di Service Desk e la comunicazione, da parte dell'operatore del servizio di assistenza da remoto, della diagnosi di massima del disservizio e previsione su modalità e tempistiche di intervento e ripristino (compreso il Severity Code).

ASPETTO DA VALUTARE	**SCOSTAMENTO TRA IL TEMPO MISURATO ED I VALORI TARGET IN RELAZIONE ALLA SEGNALAZIONE DEL DISSERVIZIO DA PARTE DELL'AMMINISTRAZIONE CONTRAENTE AL SERVIZIO DI SERVICE DESK E LA COMUNICAZIONE DELLA DIAGNOSI DI MASSIMA DEL DISSERVIZIO E PREVISIONE SU MODALITÀ E TEMPISTICHE DI INTERVENTO E RIPRISTINO**		
Unità di misura	~~Percentuale~~ Ore	**Fonte dati**	Comunicazioni Strumenti di tracciatura
Periodo di riferimento	Durata della fornitura	**Frequenza di misurazione**	Trimestrale
Dati da rilevare	T_{RISP_DIS} = Tempo di risposta al disservizio		
Regole di campionamento	Nessuna		

Formula	*IQ09* = T_{RISP_DIS} Dove: - $T_{RISP_DIS} = T_{RD_XX} – VT_{RD_XX}$ - T_{RD_XX} = tempo di risposta al disservizio misurato in ore nell'ambito della finestra di erogazione del servizio per il profilo *XX* (LP, HP). - VT_{RD_XX} = tempo di risposta al disservizio target per il profilo *XX* (LP, HP), pari a: ▪ LP: 4 ore; ▪ HP: 2 ore.
Regole di arrotondamento	La misurazione delle frazioni di ora per il parametro T_{RD_XX} avverrà secondo quanto di seguito indicato: • **per la prima ora di ritardo**, per qualsiasi frazione della prima ora, il ritardo sarà considerato pari a 1 ora; • **per le ore successive alla prima ora di ritardo:** ○ per minuti compresi tra 1-29 sarà considerato il valore orario inferiore (ad esempio se il valore misurato è pari a 132 minuti = 2,2 ore sarà considerato pari a 2 ore); ○ per minuti compresi tra 30 – 59 sarà considerato il valore orario superiore (ad esempio se il valore misurato è pari a 165 minuti = 2,75 ore sarà considerato pari a 3 ore).
Valore di soglia	*IQ09 = 0*
Azioni contrattuali	Per ogni ora eccedente la soglia prevista per l'indicatore, si applicherà la penale **"Tempo di risposta al disservizio"** pari allo **0,6‰** (zerovirgolasei per mille) dell'importo del Contratto esecutivo.
Applicazione	Amministrazione Contraente
Eccezioni	Nessuna

3.10 IQ10 – Tempestività del tempo di intervento

È definito, nell'ambito del servizio di manutenzione, come lo scostamento tra il tempo misurato ed i valori target (in base al profilo) in relazione alla segnalazione del disservizio da parte dell'Amministrazione Contraente al servizio di Service Desk e l'intervento, qualora necessario, presso la sede interessata a cura del personale tecnico messo a disposizione dall'Aggiudicatario.

ASPETTO DA VALUTARE	**SCOSTAMENTO TRA IL TEMPO MISURATO ED I VALORI TARGET IN RELAZIONE ALLA SEGNALAZIONE DEL DISSERVIZIO DA PARTE DELL'AMMINISTRAZIONE CONTRAENTE AL SERVIZIO DI SERVICE DESK E L'INTERVENTO, QUALORA NECESSARIO, PRESSO LA SEDE INTERESSATA A CURA DEL PERSONALE TECNICO MESSO A DISPOSIZIONE DALL'AGGIUDICATARIO**		
Unità di misura	~~Percentuale~~ Ore	**Fonte dati**	Comunicazioni Strumenti di tracciatura
Periodo di riferimento	Durata della fornitura	**Frequenza di misurazione**	Trimestrale
Dati da rilevare	T_{INT} = Tempo di intervento		
Regole di campionamento	Nessuna		
Formula	*IQ10* = T_{INT} Dove: - $T_{INT} = T_{I_XX} – VT_{I_XX}$ - T_{I_XX} = tempo di intervento misurato in ore nell'ambito della finestra di erogazione del servizio per il profilo *XX* (LP, HP); - VT_{I_XX} = tempo di intervento target per il profilo *XX* (LP, HP), pari al massimo quanto di seguito indicato o ai termini eventualmente migliorati in offerta tecnica: ▪ LP: 8 ore, oppure 6 ore qualora sia stato offerto il relativo migliorativo in sede di gara; ▪ HP: 4 ore, oppure 3 ore qualora sia stato offerto il relativo migliorativo in sede di gara.		
Regole di arrotondamento	La misurazione delle frazioni di ora per il parametro T_{I_XX} avverrà secondo quanto di seguito indicato: • **per la prima ora di ritardo**, per qualsiasi frazione della prima ora, il ritardo sarà considerato pari a 1 ora; • **per le ore successive alla prima ora di ritardo:** ○ per minuti compresi tra 1-29 sarà considerato il valore orario inferiore (ad esempio se il valore misurato è pari a 132 minuti = 2,2 ore sarà considerato pari a 2 ore); ○ per minuti compresi tra 30 – 59 sarà considerato il valore orario superiore (ad esempio se il valore misurato è pari a 165 minuti = 2,75 ore sarà considerato pari a 3 ore).		
Valore di soglia	*IQ10 = 0*		

Azioni contrattuali	Per ogni ora eccedente la soglia prevista per l'indicatore, si applicherà la penale **"Tempo di intervento"** pari allo **0,6‰** (zerovirgolasei per mille) dell'importo del Contratto esecutivo.
Applicazione	Amministrazione Contraente
Eccezioni	Nessuna

3.11 IQ11 – Tempestività del tempo di ripristino del servizio

È definito, nell'ambito del servizio di manutenzione, come lo scostamento tra il tempo misurato ed i valori target (in base al profilo) in relazione alla segnalazione del disservizio da parte dell'Amministrazione Contraente al servizio di Service Desk e la risoluzione dello stesso.

ASPETTO DA VALUTARE	**SCOSTAMENTO TRA IL TEMPO MISURATO ED I VALORI IN RELAZIONE ALLA SEGNALAZIONE DEL DISSERVIZIO DA PARTE DELL'AMMINISTRAZIONE CONTRAENTE AL SERVIZIO DI SERVICE DESK E LA RISOLUZIONE DELLO STESSO.**		
Unità di misura	~~Percentuale~~ Ore	**Fonte dati**	Comunicazioni Note di rilievo Strumenti di tracciatura
Periodo di riferimento	Durata della fornitura	**Frequenza di misurazione**	Trimestrale
Dati da rilevare	T_{RIPR_SER} = Tempo di ripristino del servizio		
Regole di campionamento	Nessuna		

Formula	*IQ11* = T_{RIPR_SER} Dove: - $T_{RIPR_SER} = (T_{RS_XX} – VT_{RS_XX})$~~$/VT_{RS_XX}$~~ - T_{RS_XX} = tempo di ripristino del servizio misurato in ore nell'ambito della finestra di erogazione del servizio per il profilo *XX* (LP, HP); - VT_{RS_XX} = tempo di ripristino del servizio target per il profilo *XX* (LP, HP), pari al massimo quanto di seguito indicato o ai termini eventualmente migliorati in offerta tecnica: Severity Code 1: - LP: 14 ore, oppure 12 ore qualora sia stato offerto il relativo migliorativo in sede di gara; - HP: 6 ore, oppure 4 ore qualora sia stato offerto il relativo migliorativo in sede di gara; Severity Code 2: - LP: 18 ore, oppure 16 ore qualora sia stato offerto il relativo migliorativo in sede di gara; - HP: 10 ore, oppure 8 ore qualora sia stato offerto il relativo migliorativo in sede di gara.
Regole di arrotondamento	La misurazione delle frazioni di ora per il parametro T_{RS_XX} avverrà secondo quanto di seguito indicato: • **per la prima ora di ritardo**, per qualsiasi frazione della prima ora, il ritardo sarà considerato pari a 1 ora; • **per le ore successive alla prima ora di ritardo:** ○ per minuti compresi tra 1-29 sarà considerato il valore orario inferiore (ad esempio se il valore misurato è pari a 132 minuti = 2,2 ore sarà considerato pari a 2 ore); ○ per minuti compresi tra 30 – 59 sarà considerato il valore orario superiore (ad esempio se il valore misurato è pari a 165 minuti = 2,75 ore sarà considerato pari a 3 ore).
Valore di soglia	*IQ11 = 0*

Azioni contrattuali	~~Per ogni rilievo eccedente la soglia prevista per l'indicatore, si applicherà la penale **"Tempo di ripristino del servizio"** pari allo **0,6‰** (zerovirgolasei per mille) dell'importo del Contratto esecutivo.~~ Per ogni ora di ritardo nel ripristino del servizio rispetto al tempo massimo applicabile, determinata se-condo le regole di arrotondamento previste dal presente indicatore, si applicherà la penale **"Tempo di ripristino del servizio"**, pari allo **0,6‰** (zerovirgolasei per mille) dell'importo del Contratto Esecutivo.
Applicazione	Amministrazione Contraente
Eccezioni	Nessuna

3.12 IQ12 – Tempo di disponibilità del prodotti Cloud/SaaS

L'indicatore misura la disponibilità dei prodotti Cloud/SaaS oggetto di fornitura.

Resta fermo il rispetto delle regole e dei livelli di servizio previsti dal Decreto Direttoriale ACN n. 21007/24 del 27 giugno 2024, in relazione al livello di qualificazione applicabile allo specifico prodotto Cloud/SaaS.

ASPETTO DA VALUTARE	**TEMPO DI DISPONIBILITÀ DEGLI STRUMENTI (HARDWARE E SOFTWARE) A SUPPORTO DELLA EROGAZIONE DEI SERVIZI OGGETTO DI FORNITURA.**		
Unità di misura	Minuti	**Fonte dati**	Comunicazioni Strumenti di tracciatura Strumenti di monitoraggio e controllo
Periodo di riferimento	Durata della fornitura	**Frequenza di misurazione**	Mensile
Dati da rilevare	– Intervallo di tempo di indisponibilità del prodotto non operativo (T_down) – Intervallo di tempo di riferimento (1 mese) (T_tot)		
Regole di campionamento	Nessuna		

Formula	*IQ12 = (1- (T_down/T_tot)) x 100* Dove $T_down = \sum_{j=1}^{M} dj$ Con: - M pari al numero di disservizi - d_j la durata (espressa in minuti) del disservizio j-esimo - *T_tot=(24x60X365)/12.*
Regole di arrotondamento	Ai fini del calcolo dello scostamento tra le percentuali misurate e quelle contrattuali, le prime dovranno essere arrotondate nel modo seguente: – aumento o riduzione del 0,01%: si arrotonda allo 0% per scostamenti compresi tra lo 0,0000% e 0,0049% ed al 0,01% per scostamenti superiori.
Valore di soglia	*IQ12 >= 99,98% (al netto dei fermi programmati)*
Azioni contrattuali	Per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia, si applicherà la penale **"Indisponibilità degli strumenti a supporto dei servizi"** pari allo **0,6‰ (zerovirgolasei per mille)** dell'importo complessivo del servizio di riferimento nel Contratto esecutivo di fornitura.
Applicazione	Amministrazione Contraente
Eccezioni	~~Nessuna~~ La misura del valore di soglia è effettuata al netto dei fermi programmati

3.13 IQ13 – Tempestività della comunicazione degli aggiornamenti software/firmware e delle patch di sicurezza

L'indicatore misura, per ciascun prodotto fornito, il rispetto della tempistica applicabile per la comunicazione all'Amministrazione della disponibilità di aggiornamenti software/firmware, patch di sicurezza oppure, in assenza di una correzione, misure temporanee di mitigazione pubblicate dal Vendor.

La comunicazione deve consentire all'Amministrazione di valutare la rilevanza e l'applicabilità dell'aggiornamento rispetto ai prodotti acquisiti e di decidere se richiedere al Fornitore la relativa installazione o applicazione, provvedervi autonomamente oppure tramite un soggetto terzo, o rinviarne l'esecuzione tenuto conto delle proprie esigenze operative e di continuità del servizio.

L'indicatore si applica alle attività di monitoraggio e comunicazione ricomprese nel servizio obbligatorio di monitoraggio e aggiornamento software/firmware.

ASPETTO DA VALUTARE	TEMPESTIVITÀ DELLA COMUNICAZIONE DEGLI AGGIORNAMENTI SOFTWARE/FIRMWARE E DELLE PATCH DI SICUREZZA		
Unità di misura	Ore o giorni solari.	**Fonte dati**	– Bollettini, avvisi, knowledge base e note di rilascio ufficiali del Vendor; – Portali e strumenti ufficiali messi a disposizione dal Vendor; – Alert e bollettini ACN/CSIRT Italia, ove disponibili; – Comunicazioni tra il Fornitore e l'Amministrazione; – Sistema di Trouble Ticketing; – Report di monitoraggio;

			– Ulteriori evidenze documentali.
Periodo di riferimento	Durata della fornitura del rispettivo prodotto	**Frequenza di misurazione**	Per singolo evento.
Dati da rilevare	– T_0 = data e ora in cui il Vendor pubblica o rende disponibile, attraverso i propri canali ufficiali: o l'aggiornamento software/firmware; o la patch di sicurezza; o oppure, in assenza di una correzione, la misura temporanea di mitigazione applicabile; – T_1 = data e ora in cui il Fornitore trasmette all'Amministrazione la comunicazione completa relativa all'aggiornamento software/firmware, alla patch di sicurezza o alla misura temporanea di mitigazione; – T_e = è la durata complessiva degli eventuali periodi non computabili ai sensi delle Eccezioni; – S = tempistica massima applicabile, determinata come segue: o Vulnerabilità attivamente sfruttata: 4 ore; o Vulnerabilità classificata Critical: 12 ore; o Vulnerabilità classificata High: 2 giorni solari; o Vulnerabilità classificata Medium: 3 giorni solari; o Aggiornamento software/firmware non connesso alla correzione di vulnerabilità, per il quale il Vendor segnali un impatto critico o significativo (si cita a titolo esemplificativo: sulla stabilità, sulla compatibilità, sulle prestazioni, sulla continuità operativa, sulle funzionalità di backup e ripristino oppure sulla possibilità di installare o aggiornare il prodotto): 2 giorni solari; o ulteriori aggiornamenti software/firmware, patch di sicurezza o misure temporanee di mitigazione non rientranti nei casi precedenti: 4 giorni solari. Qualora ricorrano più condizioni, si applica la tempistica più breve. La classificazione Critical, High o Medium è quella associata alla vulnerabilità nel bollettino ufficiale del Vendor, sulla base del punteggio CVSS ivi indicato. Qualora il Vendor pubblichi		

	esclusivamente la classificazione qualitativa, si applica la classe di criticità dallo stesso indicata. Per vulnerabilità attivamente sfruttata si intende una vulnerabilità per la quale il Vendor oppure l'ACN/CSIRT Italia abbia pubblicato evidenze di sfruttamento attivo.
Regole di campionamento	Nessuna
Formula	$IQ13 = T - S$ $T = T_1 - T_0 - T_e$ Dove: – T è il tempo effettivo imputabile al Fornitore per la comunicazione; – T_1 è la data e l'ora di trasmissione all'Amministrazione della comunicazione completa; – T_0 è la data e l'ora di pubblicazione o messa a disposizione dell'aggiornamento, della patch o della misura temporanea di mitigazione da parte del Vendor; – T_e è la durata complessiva degli eventuali periodi non computabili; – S è la tempistica massima applicabile.
Regole di arrotondamento	La misurazione è effettuata: – in ore, per le soglie espresse in ore; – in giorni solari, per le soglie espresse in giorni. Per la soglia espressa in ore, ogni frazione di ora eccedente comporta l'arrotondamento all'ora superiore. Per la soglia espressa in giorni, ogni frazione di giorno eccedente comporta l'arrotondamento al giorno superiore.
Valore di soglia	$IQ13 \leq 0$
Azioni contrattuali	Per ogni vulnerabilità per la quale risulti **IQ13 > 0**, per cause imputabili al Fornitore, si applica la penale **"Tempestività della comunicazione degli aggiornamenti software/firmware e delle patch di sicurezza", pari allo 0,6‰** (zerovirgolasei per mille) dell'importo del Contratto Esecutivo.
Applicazione	Amministrazione Contraente

Eccezioni	Non sono computati nel calcolo di T: – i periodi nei quali i canali ufficiali del Vendor non risultino accessibili per cause non imputabili al Fornitore, purché tale circostanza sia documentata; – i periodi derivanti dalla mancata disponibilità delle informazioni necessarie a verificare l'applicabilità dell'aggiornamento, della patch o della misura temporanea di mitigazione ai prodotti forniti, purché il Fornitore documenti di aver richiesto tempestivamente al Vendor i necessari chiarimenti; – i periodi nei quali non sia possibile trasmettere la comunicazione per cause non imputabili al Fornitore, purché le stesse siano documentate e la comunicazione sia effettuata non appena venga meno la causa impeditiva.

3.14 IQ14 – Tempestività nell'installazione o applicazione degli aggiornamenti connessi a vulnerabilità

L'indicatore misura, per ciascuna vulnerabilità che interessa i prodotti forniti, il rispetto della tempistica concordata per l'installazione o l'applicazione dell'aggiornamento o della patch di sicurezza resi disponibili dal Vendor oppure, in assenza degli stessi, della misura temporanea di mitigazione applicabile, nei casi in cui l'Amministrazione abbia richiesto al Fornitore l'esecuzione dell'intervento.

L'indicatore non si applica qualora l'Amministrazione:

- provveda autonomamente oppure tramite un soggetto terzo all'esecuzione dell'intervento;
- non autorizzi l'intervento;
- richieda di rinviare l'intervento;
- non renda disponibili nei tempi concordati gli accessi, le finestre operative o le altre condizioni necessarie alla sua esecuzione.

La tempistica è determinata tenendo conto delle caratteristiche della soluzione, del relativo modello di erogazione e, qualora l'intervento debba essere eseguito sui sistemi dell'Amministrazione, delle modalità e delle finestre operative con la stessa concordate.

L'indicatore si applica alle sole attività ricomprese nel servizio obbligatorio di aggiornamento software/firmware. Sono escluse le attività ulteriori riconducibili ai servizi opzionali di manutenzione o di supporto specialistico, anche qualora tali servizi siano stati acquistati dall'Amministrazione, per le quali trovano applicazione le rispettive modalità di esecuzione e gli specifici indicatori di qualità.

ASPETTO DA VALUTARE	TEMPO DI INSTALLAZIONE O APPLICAZIONE DEGLI AGGIORNAMENTI CONNESSI A VULNERABILITÀ		
Unità di misura	Ore o giorni solari.	**Fonte dati**	– Bollettini ufficiali del Vendor – Alert e bollettini ACN/CSIRT Italia, ove disponibili – Comunicazioni tra il Fornitore e l'Amministrazione – Sistema di Trouble Ticketing

			– Piano di Lavoro Generale – Verbali di intervento – Report o altre evidenze
Periodo di riferimento	Durata della fornitura del rispettivo prodotto	**Frequenza di misurazione**	Per singolo evento.
Dati da rilevare	– T_0 = data e ora concordate con l'Amministrazione per l'avvio dell'intervento; – T_1 = data e ora di completamento dell'installazione o dell'applicazione dell'aggiornamento, della patch di sicurezza o della misura temporanea di mitigazione applicabile; – T_e = durata complessiva dei periodi non computabili ai sensi delle Eccezioni; – S = tempistica massima applicabile in funzione della criticità della vulnerabilità o dell'eventuale sfruttamento attivo: o Vulnerabilità attivamente sfruttata: 24 ore o Critical: 72 ore o High: 7 giorni solari o Medium: 30 giorni solari La classificazione Critical, High o Medium è quella associata alla vulnerabilità nel bollettino ufficiale del Vendor, sulla base del punteggio CVSS ivi indicato. Qualora il Vendor pubblichi esclusivamente la classificazione qualitativa, si applica la classe di criticità dallo stesso indicata. Per vulnerabilità attivamente sfruttata si intende una vulnerabilità per la quale il Vendor oppure l'ACN/CSIRT Italia abbia pubblicato evidenze di sfruttamento attivo. In tale caso si applica la soglia di 24 ore, indipendentemente dal punteggio CVSS associato. La valutazione dell'impatto sistemico eventualmente indicata negli alert e nei bollettini dell'ACN/CSIRT Italia costituisce un ulteriore elemento di priorità ai fini della pianificazione dell'intervento, ma non modifica la soglia temporale applicabile. In caso di aggiornamento delle informazioni pubblicate, si tiene conto dell'ultima versione disponibile.		

Regole di campionamento	Nessuna
Formula	$IQ14 = T - S$ $T = T_1 - T_0 - T_e$ Dove: – T è il tempo effettivo imputabile al Fornitore; – T_1 è la data e l'ora di completamento dell'attività; – T_0 è la data e l'ora di decorrenza della tempistica applicabile; – T_e è la durata complessiva dei periodi non computabili; – S è la tempistica massima applicabile.
Regole di arrotondamento	La misurazione è effettuata: – in ore, per le soglie espresse in ore; – in giorni solari, per le soglie espresse in giorni. Per la soglia espressa in ore, ogni frazione di ora eccedente comporta l'arrotondamento all'ora superiore. Per la soglia espressa in giorni, ogni frazione di giorno eccedente comporta l'arrotondamento al giorno superiore.
Valore di soglia	$IQ14 \leq 0$
Azioni contrattuali	Per ogni vulnerabilità per la quale risulti **IQ14 > 0**, per cause imputabili al Fornitore, si applica la penale **"Tempestività nell'installazione o applicazione degli aggiornamenti connessi a vulnerabilità", pari allo 0,6‰** (zerovirgolasei per mille) dell'importo del Contratto Esecutivo.
Applicazione	Amministrazione Contraente
Eccezioni	Non sono computati nel calcolo di T: – i periodi dipendenti da attività, autorizzazioni, accessi o adempimenti dell'Amministrazione; – i periodi derivanti dal differimento dell'intervento disposto o concordato con l'Amministrazione per esigenze di continuità operativa; – i periodi nei quali l'installazione o l'applicazione non possa essere eseguita per cause non imputabili al Fornitore, purché tempestivamente comunicate e documentate.

4 SCHEMA PER LA PRESENTAZIONE DEI CURRICULA

Di seguito viene presentato lo schema che il fornitore dovrà utilizzare per la compilazione dei 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.

<table>
<tr><td>Nominativo</td><td colspan="3">(Inserire il Cognome e il Nome della risorsa)</td></tr>
<tr><td>Ruolo</td><td colspan="3">(Inserire il Ruolo attualmente ricoperto dalla risorsa)</td></tr>
<tr><td>Figura professionale</td><td colspan="3">(Indicazione del ruolo assegnato alla risorsa in funzione delle figure professionali richieste nel capitolato tecnico).</td></tr>
<tr><td>Servizio/attività</td><td colspan="3">(Fornire l’indicazione del servizio/attività per cui viene proposta la risorsa in relazione agli ambiti definiti nel Capitolato Tecnico)</td></tr>
<tr><td>Conoscenze</td><td colspan="3">(Fornire una breve descrizione del profilo professionale in termini di conoscenze/competenze e di aree chiave in cui la risorsa ha maturato esperienze significative)</td></tr>
<tr><td rowspan="8">Principali Esperienze Lavorative</td><td colspan="3">(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. E' necessario suddividere le esperienze per anno e per settore (Es: Pubblica Amministrazione, Bancario, Telecomunicazioni)</td></tr>
<tr><td>Settore</td><td>Data inizio-Data fine</td><td>Esperienze</td></tr>
<tr><td rowspan="3"></td><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="3"></td><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

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

Principali pubblicazioni	*(indicare le principali pubblicazioni)*	