ALLEGATO 3 – CAPITOLATO TECNICO DI APPALTO SPECIFICO

AFFIDAMENTO DI "**Cybersecurity: strumenti SWG e WAF**" MEDIANTE APPALTO SPECIFICO NELL'AMBITO DELL'ACCORDO QUADRO STIPULATO DA CONSIP PER LA FORNITURA DI PRODOTTI PER LA GESTIONE DEGLI EVENTI DI SICUREZZA E DEGLI ACCESSI, LA PROTEZIONE DEI CANALI EMAIL, WEB E DATI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI

ID 2174 – Lotto Unico

Indice

1. APPALTO SPECIFICO "CYBERSECURITY: STRUMENTI SWG E WAF"

Il presente Appalto Specifico rientra nell'ambito dell'Accordo Quadro STIPULATO DA CONSIP PER LA FORNITURA DI PRODOTTI PER LA GESTIONE DEGLI EVENTI DI SICUREZZA E DEGLI ACCESSI, LA PROTEZIONE DEI CANALI EMAIL, WEB E DATI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI

Per tutto quanto non espressamente indicato nel Capitolato Tecnico di Appalto Specifico, dovrà farsi riferimento alle previsioni del Capitolato Tecnico di Accordo Quadro (Generale e Speciale) per le parti di pertinenza, che devono intendersi quindi obbligatorie e vincolanti.

In particolare, i requisiti minimi del presente documento sono aggiuntivi ai requisiti minimi espressi in Accordo Quadro così come l'offerta migliorativa di Appalto Specifico deve essere aggiuntiva dell'offerta migliorativa di Accordo Quadro.

1.1 Definizioni

Nel corpo del presente Capitolato Tecnico, con il termine:

- **AQ** si intende l'Accordo Quadro stipulato da Consip;
- **AS** si intende il presente Appalto Specifico;
- **Amministrazione/Amministrazione Contraente**, si intende nel complesso le strutture organizzative facenti capo al Comune di Firenze, Direzione Sistemi Informativi;
- **Punto Ordinante o, brevemente, PO** l'Amministrazione richiedente l'AS sul sistema di E-Procurement di Consip;
- **CTAQ** si intende il Capitolato Tecnico Speciale dell'Accordo Quadro;
- **OEAQ** si intende l'offerta economica vincolante del Fornitore Aggiudicatario per l'AQ;
- **OTAQ** si intende l'offerta tecnica vincolante del Fornitore Aggiudicatario per l'AQ;
- **OTAS** si intende l'offerta tecnica vincolante del Fornitore aggiudicatario dell'AS, che integra e migliora l'OTAQ;
- **CTGAQ** si intende il Capitolato Tecnico Generale dell'Accordo Quadro
- **CdO** si intende il Capitolato d'oneri dell'Accordo Quadro
- **Concorrente** o **Offerente**: il RTI che partecipa alla presente gara;
- **Contratto Esecutivo**: il contratto stipulato dall'Amministrazione con il Fornitore, che si perfeziona dopo l'aggiudicazione dell'Appalto Specifico;
- **CV:** centri di valutazione del Ministero dell'interno e del Ministero della difesa;
- **CVCN:** Centro di valutazione e certificazione nazionale istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 presso l'Agenzia per la cybersicurezza nazionale;
- **Giorno lavorativo**: da lunedì a venerdì, esclusi sabato e festivi;
- **Meta-prodotto**: rappresenta l'offerta di riferimento per ogni prodotto richiesto in prima fase. Ogni meta-prodotto è caratterizzato dalla sua descrizione funzionale, da requisiti minimi, dai requisiti migliorativi offerti in prima fase e da un prezzo di riferimento che non potrà essere superato in AS, **ma non da una specifica tecnologia** (marca, modello, release firmware/software);
- **Prodotto**: rappresenta uno specifico prodotto (marca, modello, release firmware/software) offerto in seconda fase come istanza del meta-prodotto offerto in prima fase. Lo specifico prodotto offerto

avrà quindi descrizione funzionale, requisiti minimi, requisiti migliorativi del corrispondente meta-prodotto offerto in prima fase ed eventuali ulteriori requisiti migliorativi offerti in base alle richieste dell'Amministrazione Contraente. Il prezzo del prodotto non potrà superare quello del corrispondente meta-prodotto a meno di quanto espressamente previsto nel Capitolato d'Oneri;

- **Portale della fornitura**: il Portale implementato dal Fornitore aggiudicatario secondo le specifiche tecniche descritte nel Capitolato Tecnico parte Generale al paragrafo 4.1
- **Servizi Base**: i servizi, a condizioni non tutte definite, che possono essere richiesti dalle Amministrazioni a completamento della fornitura richiesta in AS, ad eccezione dei servizi inclusi nella fornitura che dovranno essere obbligatoriamente erogati;
- **Servizi Aggiuntivi**: i servizi, a condizioni da definire da parte delle Amministrazioni, che possono essere richiesti a completamento della fornitura prevista in AS. L'Amministrazione potrà valorizzare i servizi accessori secondo le regole riportate nel Capitolato d'Oneri;
- **Sistema telematico (o semplicemente "Sistema")**: indica la piattaforma telematica attraverso cui saranno gestiti gli Appalti Specifici;
- **Responsabile dell'Amministrazione:** la persona indicata dall'Amministrazione nel contratto esecutivo e individuata come interlocutore tecnico con il Fornitore per tutte le attività contrattuali.
- **Responsabile del Fornitore:** la persona indicata dal Fornitore, nell'ambito di ciascun contratto esecutivo, come referente operativo per le attività di fornitura ed erogazione dei relativi servizi connessi, i cui requisiti professionali e compiti sono descritti al par. 2.4.1.2 del Capitolato Tecnico Generale di AQ;
- **RUAC:** responsabile unico delle attività contrattuali, cioè il referente del Fornitore nei confronti di Consip S.p.A. per tutte le attività di gestione relative all'AQ, dotato di appositi poteri di firma tali da impegnare in maniera esecutiva il Fornitore nei confronti delle Amministrazioni, i cui requisiti professionali e compiti sono descritti al par. 2.4.1.1 del Capitolato Tecnico Generale di AQ;
- **Vendor/produttore**: si intende il produttore dello specifico prodotto.
- **NGFW**: apparato della tipologia Next Generation FireWall

2. CONTESTO DELL'APPALTO SPECIFICO e ELEMENTI TRASVERSALI AI VARI SERVIZI

2.1 Contesto organizzativo, tecnologico e normativo

Il Comune di Firenze è una Pubblica Amministrazione, nello specifico un ente locale. Gli enti locali sono degli enti pubblici ai quali è affidato il governo o l'amministrazione locale, ovverosia con competenza limitata entro i confini di un certo ambito territoriale. Spettano infatti al Comune tutte le funzioni amministrative che riguardano la popolazione ed il territorio comunale, precipuamente nei settori organici dei servizi alla persona e alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico, salvo quanto non sia espressamente attribuito ad altri soggetti dalla legge statale o regionale, secondo le rispettive competenze.

Il Comune di Firenze eroga servizi e svolge la propria attività amministrativa in numerose sedi distribuite sul territorio comunale e per far fronte a queste esigenze, la Direzione Sistemi Informativi (DSI) ha realizzato una complessa infrastruttura ICT. Un primo aspetto è la presenza e la gestione di una rete metropolitana in fibra ottica con velocità di connessione a gigabit, i cui nodi principali sono ormai attestati sulle decine di gigabit, che collega tra loro tutte le sedi principali e buona parte delle altre sedi minori. L'infrastruttura capillare di connettività assicura adeguati livelli di disponibilità e consente a tutti gli uffici, si tratta di oltre 3.700

postazioni di lavoro, di dialogare in modo efficiente, affidabile e sicuro con il sistema informatico centralizzato.
Il sistema informatico centralizzato fornisce oltre 2.500 servizi informatici, tra quelli di base e di alto livello, che coprono tutti gli ambiti dell'infrastruttura ICT interna (sistemi operativi, middleware, dbms, application e web server, software e proxy applicativi, programmi, web services, apps, etc.), e garantisce giornalmente elevati livelli di disponibilità, di interoperabilità, di accessibilità e di fruibilità del dato, tipici di un moderno sistema informativo basato sulla qualità della gestione dell'informazione, aspetto al quale è indispensabile collegare anche adeguati livelli di monitoraggio e controllo in ambito sicurezza informativa. Del resto, la DSI impiega una molteplicità di tecnologie per la fornitura dei servizi ed è stata già introdotta la complessità dell'attuale sistema informatico esistente nell'Ente e della dimensione del bacino di utenza, interno ed esterno, a cui sono rivolti centinaia di servizi in esso ospitati. L'obiettivo di garantire elevati livelli di disponibilità, di interoperabilità, di accessibilità, di fruibilità, di integrità e di riservatezza (ove richiesto) del dato si scontra, di fatto, con questa molteplicità di servizi, varietà di utenti e numerosità dei sistemi IT che è necessario governare al meglio; quindi, con gli impatti che questo comporta in ambito sicurezza informatica.
L'Ente, oltre ad avere numerosi servizi esposti pubblicamente, ha un'infrastruttura informatica distribuita sul territorio con un numero di utenti interni ed esterni elevato e costantemente a rischio di possibile attacco informatico. Un rischio che non si limita alla possibile interruzione di servizi verso il pubblico (cittadini, turisti, professionisti, aziende, ecc.), ma che potrebbe riguardare anche la confidenzialità, l'integrità e la disponibilità dei dati digitali gestiti e prodotti.
Ad oggi sono utilizzati alcuni degli strumenti tecnologici, già previsti in questo progetto (WAF, IPS/IDS, NGFW, …), per la protezione di parte dei siti e dei portali web oltre ai servizi digitali esposti. Tali strumenti, purtroppo, risultano sostanzialmente datati e non dispongono di funzionalità recenti e del throughput adeguato a gestire la costante crescita di servizi e dati digitali e l'incremento di traffico richiesto per gestirli ed erogarli. Di conseguenza occorre un potenziamento che, ipotizzando la disponibilità delle risorse finanziate con questo progetto, non è più opportuno procrastinare. Inoltre, gli strumenti esistenti sono basati sul classico approccio di protezione "perimetrale", mentre quelli nuovi richiesti nella presente fornitura possono essere adottati e implementati con approcci ben più resilienti e diffusi, quali lo *zero-trust-network*.
Gli ambiti o layer di I livello e i relativi obiettivi del Piano Triennale che l'Amministrazione prevede di mappare mediante le attività che saranno svolte con il Contratto esecutivo in oggetto sono:

Sicurezza Informatica	• Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA • Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

Di seguito l'indicatore di progresso identificato per l'erogazione della presente fornitura:

Denominazione	Indicatore di progresso		
Aspetto da valutare	Grado di mappatura di ciascuna classe di controlli ABSC delle misure minime di sicurezza AGID		
Unità di misura	Numero di Controlli	**Fonte dati**	Piano dei Fabbisogni o Piano di lavoro Generale
Periodo di riferimento	Momento di Pianificazione dell'intervento	**Frequenza di misurazione**	Per ogni intervento pianificato
Dati da rilevare	*N1: numero di controlli relativi alla specifica classe ABSC soddisfatti attraverso l'intervento* *NT: numero totale di controlli relativi alla specifica classe previsti dalle misure minime di sicurezza AGID*		
Regole di campionamento	Nessuna		
Formula	$Ip = (N_1 - N_0)/N_T$		
Regole di arrotondamento	Nessuna		
Valore di soglia	*N0: numero di controlli relativi alla specifica classe soddisfatti prima dell'intervento;*		
Applicazione	Amministrazione Contraente		

Tale indicatore sarà oggetto di revisione con l'Amministrazione nella fase di realizzazione della fornitura.

Si precisa che la presente procedura afferisce agli investimenti pubblici finanziati, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 (PNRR). A tal proposito si rimanda ai dettagli presenti nel capitolo 5 "ULTERIORI REQUISITI DI AS".

3. OGGETTO, DURATA DELL'APPALTO SPECIFICO E LUOGO DI ESECUZIONE

3.1 Oggetto della fornitura

Il presente AS ha ad oggetto i seguenti prodotti/servizi:

Prodotti:

1. Secure Web Gateway (SWG)
2. Web Application Firewall (WAF)

Funzionalità aggiuntive sui prodotti:

- Funzionalità aggiuntiva - SWG - Configurazione in alta affidabilità
- Funzionalità aggiuntiva - WAF - Funzionalità di bilanciamento di livello 7 (modello ISO/OSI) delle Applicazioni
- Funzionalità aggiuntiva - WAF - Configurazione in alta affidabilità

Servizi base connessi alla fornitura:

- installazione e configurazione
- formazione e affiancamento
- manutenzione profilo HP

Servizi aggiuntivi connessi alla fornitura:

- servizi professionali erogati dal vendor

Le funzionalità aggiuntive e i servizi aggiuntivi sono ricompresi nel limite del 40% della base d'asta totale di AS.

Si rimanda al paragrafo "Descrizione della fornitura" per le caratteristiche specifiche dei prodotti e servizi richiesti.

3.2 Durata del contratto

La durata del contratto è quella minima prevista dall'Accordo Quadro e pari a 12 (dodici) mesi.

3.3 Luogo di esecuzione ed orario di erogazione dei servizi

I luoghi in cui si svolgeranno le attività collegate alla presente fornitura sono:

- Via Reginaldo Giuliani, 250 – 50141 – Firenze, quale sede della Direzione Sistemi Informativi che ospita la sala primaria con gli apparati di connettività e di protezione;
- Via dell'Olmatello, 25 – 50127 – Firenze, quale sede della Protezione Civile che ospita la sala apparati di connettività e di protezione di riserva.

L'orario di erogazione dei servizi di consegna, installazione, configurazione, formazione e affiancamento sui prodotti richiesti dal presente affidamento è da lunedì a giovedì (feriali) con orario 8:30-17:30.
Per gli orari dei servizi di manutenzione, supporto, assistenza, ecc. si rimanda al relativo paragrafo.

4. DESCRIZIONE DELLA FORNITURA

4.1 Garanzia

Per la garanzia dei prodotti, il Fornitore faccia riferimento al par. 2.1.10 del CTAQ.

4.2 Prodotti

4.2.1 Requisiti del Secure Web Gateway (SWG)

Per il SWG sono richieste le seguenti fasce di prodotto:

- SWG_3 (fascia 3): fino a 10000 utenti.

Le quantità richieste per ogni fascia sono specificate nella Richiesta di Offerta.

I prodotti forniti dovranno possedere le seguenti funzionalità aggiuntive:

- Configurazione in alta affidabilità

Di seguito sono riportati i requisiti obbligatori che dovrà rispettare la soluzione :

Configurazione Minima Hardware richiesta

Sistema High port density and powerful Next-Generation Firewall in modalità ridondata di tipo modulare con seguente configurazione Hardware:

Per ciascun Appliance dovranno essere garantite almeno:

- 8 interfacce 10/100/1000 base T
- 8 interfacce SFP complete di relativo Transceiver 1000 Base LX
- 14 interfacce di tipo SFP/SFP+ (1/10 Gbps) equipaggiate con moduli SFP Fibra ottica SR 10/1 Gbps autosense
- Possibilità di equipaggiare moduli con ciascuno 2 porte da 40 Gbps
- Doppio SSD almeno da 1 TB in RAID 1
- Funzionalità di Breach fighter (sandboxing) e advanced antivirus
- Mandatorio disporre di un'interfaccia IPMI per la gestione remota dell'hardware, questa funzione è indispensabile per ottenere una gestione completa dell'hardware da remoto, monitorare le componenti e controllare completamente l'appliance (control, reboot, interruption, etc.). Questa interfaccia deve essere operativa a prescindere dallo stato del firewall e della relativa configurazione.

Performance Minime richieste:

- Firewall throughput (1518 byte UDP) 170 Gbps
- Firewall throughput (IMIX**) 53.3 Gbps
- IPS throughput (1518 byte UDP) 68 Gbps
- IPS throughput (1 MByte HTTP files) 27 Gbps
- Antivirus throughput 12.5 Gbps

VPN :

- IPSec throughput - AES-GCM 20 Gbps
- IPSec throughput - AES256/SHA2 12.3 Gbps
- Max number of IPSec VPN tunnels 10,000
- Max number of SSL VPN (Portal mode) 2,048
- Number of simultaneous SSL VPN clients 500

NETWORK CONNECTIVITY:

- Concurrent connections 20,000,000 New connections per second 250,000
- Number of main gateways (max)/backup (max) 64/64

Struttura Modulare con almeno 7 slot di cui almeno 3 non popolati per uso futuro, in grado di gestire una combinazione di porte come segue al fine di poter gestire l'evoluzione della rete e delle necessità che dovessero emergere:

- 10/100/1000 interfaces 8-64
- 10 Gb copper interfaces 0-32
- 1 Gb fiber interfaces 0-64
- 10 Gb fiber interfaces 22-34
- 40 Gb fiber interfaces 0-16

SYSTEM

- Number of rules (recommended / specific configuration) 8192 / 32768
- Max Number of static routes 10240

REDUNDANCY

- High Availability (Active/Passive)
- Redundant SSD RAID 1
- Redundant power supply (hot swappable)
- Redundant ventilation (hot swappable)

MTBF non inferiore a 20 anni a 25gradi centigradi

Compliance CE/FCC/CB

Certificazione Europea ANSSI e BSI

Visto la particolare criticità dei prodotti richiesti e la tipologia di dati e informazioni che dovranno proteggere, è richiesta la totale assenza di backdoor e di funzionalità non compatibili con il regolamento GDPR Europeo, in particolare il prodotto deve risultare non soggetto a legge federale USA Cloud ACT e Patriot ACT, o di qualsiasi altro ente non espressamente autorizzato.
Il Cloud ACT è per l'accesso ai dati fuori dagli US. "Clarifying Lawful Overseas Use of Data (CLOUD) Act" che consente alle autorità US, forze dell'ordine e agenzie di intelligence federali e nazionali, di acquisire dati informatici dagli operatori di servizi di cloud computing a prescindere dal posto dove questi dati si trovano; quindi, anche se sono su server fuori dagli Usa.
Il "Patriot ACT" rinforza il potere dei corpi di polizia e di spionaggio statunitensi, quali CIA, FBI e NSA per ridurre il rischio di attacchi terroristici negli Stati Uniti, tramite la possibilità di effettuare intercettazioni telefoniche, l'accesso a informazioni personali e il prelevamento delle impronte digitali, ed eseguire le intercettazioni del traffico Internet, senza un mandato della magistratura e una notifica ai diretti interessati del materiale acquisito.

Gestione in modo indipendente per interfaccia tra protezione applicata a livello 2 (bridging) e L3 routing.

Nel L2, deve essere garantita l'applicazione del filtro FW, IPS e IDS tra VLAN e interfacce fisiche che presentano lo stesso piano di indirizzamento a livello 2, lo stesso tipo di protezione dovrà poter essere applicato anche in combinazione con Interfacce o VLAN in routing. (questa condizione è indispensabile al fine di poter mantenere l'attuale assetto e disegno dell'infrastruttura di rete e di sicurezza).

Gestione del reindirizzamento intelligente tra network presenti sulle interfacce, nel caso in cui due network siano presenti e configurate sulle interfacce fisiche o virtuali, il firewall provvederà a gestire direttamente i pacchetti a prescindere dal gateway impostato sui client stessi.

Supporto del Layer 2 Extension su VPN, dovrà essere possibile estendere il livello 2 di una network anche a livello geografico incapsulandolo all'interno di VPN IPSEC.

Funzionalità di return route, un pacchetto che entra all'interno del firewall produrrà la relativa riposta sulla stessa interfaccia di ingresso, questa funzione consente di poter avere più regole di port forwarding su diverse connessioni geografiche e gestire le relative risposte senza necessità di stabilire rotte specifiche che creerebbero criticità in processi di alta affidabilità.

Gestione di diverse tipologie di configurazioni in base a modelli applicabili in combinazione e senza necessità di riavvio del firewall stesso, attuale concetto di slot, dove è possibile creare almeno fino a 10 profili di configurazione a livello di Filtri, NAT, IPS, Application Protecion Proxy e SMTP Filter tra cui swappare in funzione delle esigenze o applicare in modo combinato.

Almeno tre livelli di Policy organizzate in ordine di priorità, Implicita, Globale e Locale, queste ultime due gestibile con almeno 10 profili diversi.

Gestione aggregazione interfacce in modalità LACP con possibilità di creare bridge a livello due anche tra Aggregazioni diverse in LACP.

Indicazione Routing definibile in modalità PBR (Policy-Based Routing) per singola regola con possibilità di modificare lo stesso in base alla fascia oraria definendo piu orari per giorno della settimana.

Filtri gestibili in base a reputation, applicazione, servizio, geolocalizzazione.

Servizio di Vulnerability Manager che sia in grado di individuare la presenza di possibili Vulnerabilità degli host in base al passaggio del traffico specifico attraverso il Firewall.

In questi casi dovrà essere messo a disposizione un portale accessibile da Browser e protetto da connessione SSL dove dovrà essere possibile verificare:

- Le liste delle vulnerabilità con CVE che possono esser individuate dalla procedura di analisi del sistema.
- Il database dell'IP Reputation, con possibilità di effettuare delle query in base all'IP/Domain

USAGE CONTROL

- Firewall/IPS/IDS mode
- Identity-based firewall
- Application detection and management
- Microsoft Services Firewall
- Industrial firewall/IPS/IDS
- Industrial application control
- Detection and control of the use of mobile terminals
- Application inventory
- Vulnerability detection
- Geolocation (countries, continents)
- Dynamic Host Reputation
- URL filtering (embedded database or cloud mode)
- Transparent authentication (Active Directory, SSO Agent, SSL, SPNEGO)
- Multiuser authentication in cookie mode (Citrix-TSE)
- Guest and sponsorship mode authentication, webservices

PROTECTION FROM THREATS

- Intrusion detection and prevention
- Protocols autodetection and compliancy check
- Application inspection
- Protection from denial of service attacks (DoS)
- Protection from SQL injections
- Protection from Cross-Site Scripting (XSS)
- Protection from malicious Web2.0 code and scripts (Clean & Pass)
- Trojan detection
- Detection of interactive connections (botnets, Command&Control)
- Protection from data evasion
- Advanced management of fragmentation
- Automatic reaction to attack (notification, quarantine, block, QOS, dump)
- Antispam and antiphishing:
- reputationbased analysis, heuristic engine
- Embedded antivirus (HTTP, SMTP, POP3, FTP)
- SSL decryption and inspection - VoIP protection (SIP)
- Collaborative security: IP reputation
- Cloud based Sandbox on the European territory (option)
- Traffic Geolocalization

CONFIDENTIALITY

- Site-to-site or nomad IPSec VPN
- Remote SSL VPN access in multi-OS tunnel mode (Windows, Android, iOS, etc.)
- SSL VPN agent with automatic configuration (Windows)
- Support for Android/ iPhone IPSec VPN

NETWORK - INTEGRATION

- IPv4 e IPv6
- NAT, PAT, transparent (bridge)/routed/hybrid modes
- Dynamic routing (RIP - OSPF - BGP) - Multiple link management (balancing, failover)
- Multi-level internal or external PKI management
- Multi-domain authentication (including internal LDAP)
- Explicit proxy
- Policy-based routing (PBR)
- QoS management
- DHCP client/relay/server
- NTP client
- DNS proxy-cache
- HTTP proxy
- LACP management che dovrà esser consentito in caso di aggregazione di interfacce indispensabile per l'associazione allo stack degli switch di core presenti
- Spanning-tree management (RSTP/ MSTP)
- SD-WAN
- Multifactor Authentication (MFA)

MANAGEMENT strutturato sui seguenti livelli

- Web-based management

- Interface with privacy mode (GDPR compliant)
- Object-oriented security policy
- Contextual security policy
- Real-time configuration helper
- Rule counter
- Multiple installation wizards
- Global/local security policy
- Embedded log reporting and analysis tools
- Interactive and customizable reports
- Support for multiple syslog server UDP/TCP/TLS - SNMP v1, v2c, v3 agent - IPFIX
- Automated configuration backup
- Open API
- Script recording

LOG SERVER (RIDONDATO)

2 istanze licenziate e contemporanee di Log Supervisor, installabile su piattaforma vmWare, con certificazione EAL3+ che deve garantire:

- Advance log analysis
- Compliance years of legal archive
- Report manual & automatic
- Central Log Management

Visibilità globale:

- Dashboard, report e avvisi
- Ricerca multicriterio
- Rapporti di attività
- Funzione di ricerca come da caratteristiche di seguito riportate

Scalabilità:

- Elevato volume di firewall gestibile previa semplice acquisizione di licenza al fine di garantire una espansione su altri dispositivi presenti
- Gestione di numerosi registri per più anni
- Alta disponibilità

Gestione degli incidenti

- Definizione delle regole di allerta
- Assegnazione degli avvisi

LOG MANAGEMENT

- Event collection via syslog (TCP & UDP)
- Secure collection via syslog-TLS
- Syslog Forwarder function
- Events Per Second (EPS): 10,000+
- Normalisation and native indexing of SNS & SES logs
- Log management over multiple years (1+ years)
- Number of firewalls: 500+

SEARCH TYPES

- Simple search
- Multicriteria advanced search (log type, time, etc.)

- Predefined searches
- Results displayed as raw logs, normalised logs and graphical logs
- Enrichment with external sources (CSV, IPtoHost, LDAP, GeoIP)
- Navigation through time (minutes, hours, days, specific time range)
- Search history
- Results exported in CSV format

ALERTS AND INCIDENT MANAGEMENT

- Automatic generation based on pre-established rules
- Management of alert criticality (4 levels)
- Incidents assigned to administrators for resolution, with resolution tracking REPORTS
- Manual or automatic generation (hour, day, week or month)
- Customised layout or predefined templates
- Report format: PDF, HTML, XLS, DOCX, CSV
- Reports sent by email

I requisiti migliorativi oggetto di valutazione di AS e riportati anche nella richiesta d'Offerta sono di seguito elencati:

AS 4.1 Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)

Allo stato attuale è presente una coppia di apparati NGFW (Next Generation FireWall del produttore Stormshield, modello SN6000) in modalità active-standby, distribuita sui due siti indicati al paragrafo 3.3, che svolge funzionalità avanzate di protezione quali deep inspection, stateful control, intrusion detection e intrusion protection. Tali apparati assicurano una segmentazione della rete con combinazioni di politiche di filtro applicate su Layer 2 e Layer 3 sia per interfacce fisiche per VLAN associate alle interfacce stesse senza alcuna limitazione di combinazione. È intenzione dell'Amministrazione procedere alla sostituzione degli apparati descritti, prossimi all'obsolescenza, con una soluzione in grado di migrare le attuali regole di protezione e le configurazioni di rete con il minimo impatto possibile sulla disponibilità dei servizi erogati o addirittura assicurare una migrazione del tutto trasparente per servizi ed utenti; garantendo, allo stesso tempo, con i nuovi apparati SWG le funzionalità ad oggi presenti e giudicate irrinunciabili per la sicurezza e il mantenimento della attuale organizzazione dell'infrastruttura.

AS 4.2 Configurazione della soluzione in alta affidabilità.

Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto. Come descritto nel precedente paragrafo, l'attuale coppia di NGFW è configurata in modalità active-standby, quindi la nuova soluzione SWG offerta deve prevedere un livello di alta affidabilità che garantisca una resilienza non inferiore a quanto già esistente.

4.2.2 Requisiti del Web Application Firewall (WAF)

Per il WAF sono richieste le seguenti fasce di prodotto:

- WAF_2 (fascia 2): fino a 5 Gbps di throughput HTTP.

Le quantità richieste per ogni fascia sono specificate nella Richiesta di Offerta.

I prodotti forniti dovranno possedere le seguenti funzionalità aggiuntive:

- Funzionalità di bilanciamento di livello 7 (modello ISO/OSI) delle Applicazioni

- Configurazione in alta affidabilità

Di seguito sono riportati i requisiti obbligatori che dovrà rispettare la soluzione :

- Protezione SIA dagli “OWASP Top 10 Web Application Risks” SIA dagli “OWASP Top 10 API Security Risks” (questa nuova catalogazione elaborata da OWASP è molto importante perché rappresenta una nuova e pericolosa categoria di attacchi di nuova generazione focalizzati sulle API, ormai dominanti negli applicativi Web di nuova generazione
- Disponibilità sia di funzionalità di API Discovery (JSON e XML), che di funzionalità di API Security nella soluzione (JSON e XML)
- Protezione BOT avanzata, quindi non solo legata a Database di BOT conosciuti, ma anche alla disponibilità di un ambiente di Intelligenza Artificiale/Machine Learning nel cloud del Vendor
- Protezione non solo da attacchi DDOS di tipo Applicativo, ma anche da attacchi DDOS di tipo Volumetrico
- Protezione completa in relazione all’Upload di file verso gli applicativi Web, vale a dire disponibilità sia di una protezione Antivirus/Antimalware “signature” based, sia di un ambiente di Advanced Threat Protection basato su Sandbox nel cloud del Vendor
- Utilizzo delle Smart Signatures sviluppate dal Vendor. Tali signatures vengono raggruppate in “gruppi” per consentire una significativa ottimizzazione della memoria e velocità di rilevamento rispetto alle signatures “statiche”. Ogni signature all’interno di un gruppo ha la capacità di rilevare gli attacchi trovati in 40 signatures standard, e questo è un netto vantaggio se comparato con la tipica sicurezza basata su firma disponibile con altri WAF, in cui ogni firma è specifica per una vulnerabilità o un attacco e la loro corrispondenza richiede molto tempo.
- Pieno supporto per l’Identity e l’Access Control; quindi, supporto non solo di utenti/gruppi locali, ma soprattutto supporto LDAP/AD. Radius, Kerberos v5, SMS Passcode, OKTA, SAML, Azure AD, DUO, RSA Secure ID, OpenID Connect, JWT arrivando fina al supporto MFA
- Disponibilità di un tool gratuito ed integrato per fare dei Vulnerability Scanner, da poter usare anche come Automatic Remediation Service
- Virtual Patching integrabile con più di 20 differenti Vulnerability Scanners
- Pieno supporto della Client-Site Protection per la difesa contro gli attacchi alla Supply Chain delle aziende
- Protezione sia dal furto di informazioni relative alla struttura degli applicativi Web (Website Cloaking) sia dal furto di dati sensibili (Outbound Data Theft Protection)
- Possibilità non solo di bloccare attacchi geograficamente identificati (Geo IP), ma anche categorizzati all’interno di DataBase costantemente aggiornati (nodi TOR per esempio, piuttosto che Proxies pubblici, etc.)
- Completo supporto di funzionalità di Application Delivery Control; nella fattispecie supporto di TLS/SSL Offloading, Load Balancing, Content Routing, Caching e Compressione, supporto di soluzioni di HSM come Gemalto, supporto IPv6, supporto FTP/S, Website e URL Translation
- Possibilità di esportazione dei log tramite Syslog e piena integrazione con le più diffuse piattaforme SIEM/SOAR (Splunk, ARCsight, Azure Sentinel, RSA enVision, IBM Qradar, Symantec, Sumologic, Loggly, Azure Event Hub ed altre ancora)
- La soluzione WAF deve essere disponibile per l’installazione on-prem, sia in modalità HW-based che Virtual-based e, nell’ottica di possibili progetti futuri, deve essere anche disponibile sui più diffusi Cloud pubblici come AWS, Google Cloud e Microsoft Azure oltre ad essere disponibile in modalità WAF-as-a-Service (su Cloud del produttore stesso)
- La soluzione deve essere riconosciuta come “Strong-Performer” dal Forrester Wave dedicato alle soluzioni WAF

I requisiti migliorativi oggetto di valutazione di AS e riportati anche nella richiesta d'Offerta sono di seguito elencati:

AS 8.1 Qualità e Innovatività del Sistema di apprendimento automatico basato su Machine Learning del comportamento applicativo, in grado di rilevare le azioni che si discostano dal comportamento applicativo appreso, riducendo i falsi positivi

AS 8.2 Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)

Allo stato attuale è presente una coppia di apparati bilanciatori (load balancer del produttore Barracuda modello ADC 540) in modalità active-standby, distribuita sui due siti indicati al paragrafo 3.3, che svolge funzionalità avanzate di bilanciamento dei servizi e base di protezione quali intrusion detection e intrusion protection. È intenzione dell'Amministrazione procedere alla sostituzione degli apparati descritti, prossimi all'obsolescenza, con una soluzione in grado di migrare le attuali regole di protezione e le configurazioni di bilanciamento con il minimo impatto possibile sulla disponibilità dei servizi erogati o addirittura assicurare una migrazione del tutto trasparente per servizi ed utenti; garantendo, allo stesso tempo, con i nuovi apparati WAF le funzionalità ad oggi presenti e giudicate irrinunciabili per la sicurezza e il mantenimento della attuale esposizione di applicativi e siti bilanciati con un maggior livello di protezione e resilienza.

AS 8.3 Configurazione della soluzione in alta affidabilità.

Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto. Si veda quanto già precisato nel presente paragrafo.

AS 8.4 Efficacia delle funzionalità aggiuntive di bilanciamento del carico a livello 7 rispetto alle minime richieste dalla PA e/o relative modalità di implementazione.

AS 8.5 Supporto standard PCI DSS.

AS 8.6 Modalità di implementazione, varietà e numerosità delle policy/eccezioni alle policy associabili ad applicazioni in essere presso la PA al fine di semplificare la gestione in sicurezza degli applicativi.

4.3 Servizi

Servizi SWG

Oltre ai servizi base sopra indicati la soluzione di SWG dovrà prevedere i servizi aggiuntivi erogati dal Vendor di seguito riportati:

- Ampliamento della capacità di Log da 250 GB a 1 TB;
- Manutenzione con Supporto H24 da parte TAC (Technical Assistance Center) del produttore erogato attraverso personale certificato;
- Manutenzione di tipo H24 7/7 con risposta da parte di un tecnico entro 10 minuti dalla apertura del ticket
- Supporto Vulnerability manager
- Supporto Host Reputation

Si richiede inoltre la migrazione della attuale configurazione presente sui Next Generation FireWall (NGFW) sulla nuova infrastruttura, a tale scopo il personale che opererà sull'infrastruttura dovrà avere il massimo livello di certificazione per entrambi in prodotti sia quello attualmente presente che il nuovo prodotto.
In particolare, per l'attuale sistema, una certificazione di tipo CSNTS (Certified Stormshield Network Troubleshooting & Support) rilasciata ufficialmente dal produttore da almeno 5 (cinque) anni con i relativi rinnovi periodici in corso di validità, accompagnata da una dichiarazione ufficiale da parte del produttore stesso. Questo al fine di gestire la completa migrazione delle configurazioni e dei servizi che nel tempo sono

stati implementati: per fare questo con elevati livelli di qualità e senza possibilità di errore, vista la complessità delle configurazioni presenti è necessario disporre della massima competenza.
Il pacchetto relativo al supporto tecnico dovrà essere garantito nei 12 mesi successivi al collaudo con modalità H24 7/7 con prima risposta del personale Tecnico entro 10 minuti dall'apertura della chiamata e con intervento on site entro le 2 ore in caso di guasto bloccante sempre di un tecnico con il massimo profilo di certificazione tecnica (non commerciale) avvallata da dichiarazione ufficiale del produttore.

Servizi WAF

Oltre ai servizi base sopra indicati la soluzione di WAF dovrà prevedere i servizi aggiuntivi erogati dal Vendor di seguito riportati:

- Manutenzione 12 mesi di tipo H24 7/7 con risposta da parte di un tecnico entro 15 minuti dalla apertura del ticket e intervento on site entro 2 ore in caso di guasto bloccante

Requisiti migliorativi

I requisiti migliorativi oggetto di valutazione di AS e riportati anche nella richiesta d'Offerta sono di seguito elencati:

AS 9.1 Ulteriori competenze ed esperienze specifiche del personale addetto ai servizi (ad eccezione del supporto specialistico)

AS 9.2 Certificazioni Vendor Neutrali Aggiuntive del personale addetto ai servizi (ad eccezione del supporto specialistico)

AS 9.3 Certificazioni di tipo sales o technical del personale addetto ai servizi sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase (ad eccezione del supporto specialistico)

AS 9.4 Misure premiali volte a promuovere l'assunzione di giovani e donne, l'inclusione lavorativa delle persone disabili, la parità di genere e le ulteriori misure di conciliazione vita lavoro, indicate in conformità a quanto previsto dall'art. 47, comma 5, Decreto Legge 31 maggio 2021 n. 77. Quelle previste per questo AS e che daranno diritto a punteggio sono (ciascuno, se presente, pari a 0,20 punti – si veda la tabella presente nel paragrafo 3.1 del documento "Richiesta d'offerta" per i dettagli):

- Possesso della certificazione di responsabilità sociale ed etica SA 8000 o equivalente;
- Imprese o start-up di cui siano titolari persone con disabilità o di cui la maggioranza dei soci siano persone con disabilità o che abbiano persone con disabilità nel ruolo di presidente, amministratore delegato, direttore generale.
- Previsione nell'organico aziendale della figura del *disability manager*;
- Imprese o cooperative sociali il cui direttivo è costituito per la maggioranza da giovani tra i diciotto e i trentacinque anni;
- Imprese o start-up in cui la compagine societaria sia composta, per oltre la metà numerica dei soci e di quote di partecipazione, da soggetti di età inferiore ai 36 anni.

AS 9.5 Architettura e modalità di implementazione del collegamento (qualora questo non sia messo a disposizione dalla PA) per l'accesso remoto ai sistemi dell'Amministrazione a supporto delle attività di manutenzione, al fine di garantire l'integrità, la riservatezza e la sicurezza dei dati.

AS 9.6 Modelli organizzativi, modalità operative e strumenti adottati per l'erogazione dei servizi aggiuntivi ai fini di dimostrare il soddisfacimento dei livelli di servizio offerti dal Concorrente e ottimizzare i tempi di rilascio dei deliverable attesi

5. ULTERIORI REQUISITI DI AS

Art. 47 del DL 77/2021

Il presente appalto, in quanto rientrante nei programmi cofinanziati dai fondi strutturali dell'Unione europea ricade nell'ambito di applicazione dell'art. 47 del Decreto Legge 31 maggio 2021, n. 77, convertito in Legge n. 108 del 29 luglio 2021, e delle Linee Guida di cui al D.P.C.M., Dipartimento per le Pari Opportunità, del 7 dicembre 2021, che perseguono le finalità stabilite dal citato art. 47. Pertanto, all'operatore che partecipa alla presente procedura sono applicabili i requisiti necessari di seguito elencati:

1. **Rapporto sulla situazione del personale per operatori economici che occupano oltre 50 dipendenti (art. 47, comma 2 dl 77/2021)**. Ai sensi dell'art. 47, comma 2, del DL 31/05/2021, n. 77, convertito con modificazioni dalla L. 108/2021, gli operatori economici tenuti alla redazione del rapporto sulla situazione del personale, ai sensi dell'art. 46 del D. Lgs 11/04/2006, n. 198, producono, a pena di esclusione, al momento della presentazione della offerta, copia dell'ultimo rapporto redatto, con attestazione della sua conformità a quello eventualmente trasmesso alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità, ovvero, in caso di inosservanza dei termini previsti dal comma 1 del medesimo art. 46, con attestazione della sua contestuale trasmissione alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità.

2. **Assolvimento degli obblighi in materia di lavoro delle persone con disabilità (art. 47, comma 4 dl 77/2021).** Ai sensi dell'art. 17, L. 12/03/1999, n. 68, le imprese, pubbliche o private, sono tenute a presentare, a pena di esclusione, al momento della presentazione dell'offerta la dichiarazione del legale rappresentante che attesti di essere in regola con le norme che disciplinano il diritto al lavoro delle persone con disabilità. Costituisce altresì causa di esclusione dalla procedura il mancato rispetto, al momento della presentazione dell'offerta, degli obblighi in materia di lavoro delle persone con disabilità di cui alla L. 12/03/1999, n. 68.

3. **Assolvimento dell'obbligo di consegna della relazione di genere sulla situazione del personale maschile e femminile (per operatori economici che occupano un numero pari o superiore a 15 e non superiore a 50 dipendenti) in precedenti appalti finanziate con risorse del PNRR, PNC o fondi strutturali dell'unione europea (art.47, comma 6 dl 77/2021).** Ai sensi dell'art. 47, comma 6 del decreto legge n. 77 del 2021 sono esclusi dalla presente procedura gli operatori economici che occupano un numero di dipendenti pari o superiore a quindici e non superiore a cinquanta, che nei dodici mesi precedenti al termine di presentazione dell'offerta hanno omesso di produrre alla stazione appaltante di un precedente contratto d'appalto, finanziato in tutto o in parte con i fondi del PNRR, del PNC o fondi strutturali europei, la relazione di cui all'articolo 47, comma 3 del decreto legge n. 77 del 2021. Pertanto detti operatori economici sono tenuti a presentare, a pena di esclusione, al momento della presentazione dell'offerta, apposita dichiarazione del legale rappresentante che attesti di non essere stato aggiudicatario di precedenti contratti di appalto finanziati in tutto o in parte con i fondi del PNRR, del PNC o Fondi strutturali dell'Unione Europea o, in caso contrario, di aver prodotto alle relative stazioni appaltanti nei dodici mesi precedenti al termine di presentazione dell'offerta del presente appalto la relazione di genere di cui al citato articolo 47, comma 3. Qualora non ricorrano le condizioni, la Ditta dovrà presentare una dichiarazione motivando le ragioni per le quali non è tenuta agli adempimenti precedenti.

4. **Obblighi di assunzione per l'occupazione giovanile e femminile (art. 47, comma 4 dl 77/2021).** Ai sensi dell'art. 47, comma 4, del DL 31/05/2021, n. 77, convertito con modificazioni dalla L. 108/2021, l'Operatore Economico dichiara in sede di presentazione dell'offerta di assumere l'obbligo di assicurare, in caso di affidamento del contratto, una quota pari almeno al 30% (trenta per cento) delle assunzioni necessarie per l'esecuzione del contratto o per la realizzazione di attività ad esso connesse o strumentali, sia all'occupazione giovanile sia all'occupazione femminile.

Pertanto, l'ulteriore documentazione obbligatoria richiesta è la seguente:

1. **Se operatore economico che occupa oltre 50 dipendenti, i documenti e le dichiarazioni di cui al punto 1 del precedente paragrafo** e cioè:

• copia dell'ultimo rapporto sulla situazione del personale redatto ai sensi dell'art. 46 del D.Lgs. 11/04/2006, n. 198, nonché

• attestazione della sua conformità a quello trasmesso alle rappresentanze sindacali aziendali e della consigliera e al consigliere regionale di parità

ovvero, in caso di inosservanza dei termini previsti dal comma 1 dell'art. 46 del D.Lgs. 11/04/2006, n. 198

• attestazione della sua contestuale trasmissione alle rappresentanze sindacali aziendali e della consigliera e al consigliere regionale di parità.

In ogni caso la copia dell'ultimo rapporto e l'attestazione allegata devono essere prodotti e sottoscritti dal legale rappresentante (o procuratore) dell'operatore economico, e, nel caso di raggruppamenti temporanei, da tutti gli operatori economici che partecipano alla procedura in forma congiunta (se tenuti all'obbligo di cui al citato art. 46).

2. **La dichiarazione di cui al punto 2 del precedente paragrafo** e cioè dichiarazione di essere in regola con le norme che disciplinano il diritto al lavoro delle persone con disabilità, ai sensi dell'art. 17, L. 12/03/1999, n. 68. La dichiarazione deve essere prodotta e sottoscritta dal legale rappresentate (o procuratore) dell'operatore economico, e (se tenuti all'obbligo), nel caso di raggruppamenti temporanei, da tutti gli operatori economici che partecipano alla procedura in forma congiunta.

3. **La dichiarazione di cui al punto 3 del precedente paragrafo** e cioè la dichiarazione di assumere l'obbligo di assicurare, in caso di affidamento del contratto, una quota pari almeno al 30 per cento delle **assunzioni necessarie** per l'esecuzione del contratto o per la realizzazione di **attività ad esso connesse o strumentali**, sia all'occupazione giovanile sia all'occupazione femminile. La dichiarazione deve essere prodotta e sottoscritta dal legale rappresentante (o procuratore).
Si precisa che in caso di affidamento del presente appalto l'Operatore Economico dovrà compilare e produrre a richiesta della Stazione Appaltante, prima della stipula del contratto, uno schema di organizzazione del personale che sarà impiegato nell'appalto, con indicazione in dettaglio delle assunzioni ai sensi dell'articolo 47 del Decreto Legge 77/2021. In particolare, lo schema dovrà illustrare l'entità del personale impiegato nell'esecuzione dello stesso e le concrete modalità di applicazione della clausola relativa all'assunzione di giovani, con età inferiore a trentasei anni e donne, con particolare riferimento a inquadramento, trattamento economico, qualificazione professionale.

4. **La dichiarazione di cui al punto 4 del precedente paragrafo (per gli operatori economici che occupano un numero pari o superiori a quindici dipendenti e non tenuti alla redazione del rapporto sul personale ai sensi dell'art. 46 del D.Lgs. 11 aprile 2006, n.198)** e cioè alla dichiarazione del legale rappresentante che attesti di non essere stato aggiudicatario di precedenti contratti di appalto finanziati in tutto o in parte con i fondi del PNRR, del PNC o Fondi strutturali dell'Unione Europea o, in caso contrario, di aver prodotto alle relative stazioni appaltanti nei dodici mesi precedenti al termine di presentazione dell'offerta del presente appalto la relazione di genere di cui al citato articolo 47, comma 3.

Infine, le ulteriori condizioni di esecuzione a carico dell'affidatario sono le seguenti:

1) Assolvimento di consegna della relazione di genere sulla situazione del personale maschile e femminile (art. 47, comma 3, dl 77/2021).

Ai sensi dell'art. 47, comma 3, del decreto legge n. 77 del 2021 gli operatori economici che occupano un numero pari o superiore a quindici dipendenti e non tenuti alla redazione del rapporto sulla situazione del personale, ai sensi dell'art, 46 del d.lgs. 11 aprile 2006, n. 198, sono tenuti, entro sei mesi dalla conclusione del contratto, a consegnare alla stazione appaltante una relazione di genere sulla situazione del personale maschile e femminile in ognuna delle professioni ed in relazione allo stato di assunzioni, della formazione, della promozione professionale, dei livelli, dei passaggi di categoria o di qualifica, di altri fenomeni di mobilità dell'intervento della Cassa integrazione guadagni, dei licenziamenti, dei prepensionamenti e pensionamenti, della retribuzione effettivamente corrisposta.
L'operatore economico è altresì tenuto a trasmettere la relazione alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità.
La mancata produzione della relazione comporta l'applicazione di una **sanzione giornaliera pari allo 0,6 per mille dell'ammontare netto contrattuale**, entro l'importo massimo del 20% di tale ammontare netto, nonché l'impossibilità di partecipare in forma singola o in raggruppamento temporaneo, per un periodo di 12 mesi, ad ulteriori procedure di affidamento afferenti agli investimenti finanziati con le risorse derivanti da PNRR, PNC e altri fondi europei.

2) Relazione sull'avvenuto assolvimento degli obblighi relativi al diritto al lavoro delle persone con disabilità.
Ai sensi dell'art. 47, comma 3-bis, del DL 31/05/2021, n. 77, convertito, con modificazioni, dalla L. 29/07/2021, n. 108, gli operatori economici sono tenuti, entro sei mesi dal perfezionamento del contratto, a consegnare alla stazione appaltante la certificazione di cui all'articolo 17 della legge 12 marzo 1999, n. 68, e una relazione che chiarisca l'avvenuto assolvimento degli obblighi previsti a carico delle imprese dalla L. 12/03/1999, n. 68, e illustri eventuali sanzioni e provvedimenti imposti a carico delle imprese nel triennio precedente la data di scadenza di presentazione dei preventivi. L'operatore economico è altresì tenuto a trasmettere la relazione alle rappresentanze sindacali aziendali. **La mancata produzione della relazione comporta l'applicazione di una sanzione giornaliera** pari allo 0,6 per mille dell'ammontare netto contrattuale, entro l'importo massimo del 20% di tale ammontare netto. Le penali di cui ai punti precedenti non possono comunque superare, complessivamente il 20% dell'ammontare netto contrattuale.

<u>Principio DNSH</u>

Trattandosi di fornitura finanziata tramite fondi PNRR, per gli apparati oggetto del presente appalto, l'Amministrazione richiede:

- il pieno rispetto dei requisiti tecnici e ambientali previsti (DNSH – Do Not Significant Harm), sulla base della Circolare RGS n. 32 del 30 dicembre 2021 e dell'art. 17 del Regolamento UE 852/2020, che costituiscono dei requisiti minimi, il cui mancato rispetto, stante il carattere mandatorio, comporterà l'esclusione dalla gara;
- la documentazione a comprova del rispetto dei suddetti requisiti. Tale prova è fornita mediante la compilazione e il rispetto delle certificazioni richieste dalla checklist, per ciascuna diversa tipologia di apparato offerto, quindi una per l'SWG e una per il WAF. La checklist è presente nell'allegato denominato: "Checklist 3_Acquisto, Leasing e Noleggio di computer e AEE.xlsx"

6. LIVELLI DI SERVIZIO E PENALI

Trovano applicazione i livelli di servizio e penali già previsti nel CTAQ.

Si prevede anche le seguenti penali per questo AS:

P1 - Inadeguatezza parti di ricambio e/o carenze tecnico-professionali e/o qualitative nell'espletamento della fornitura; qualora le modalità di intervento adottate, le procedure rilevate, il personale tecnico e/o le parti in sostituzione impiegati dal fornitore non risultino adeguati/pertinenti/funzionanti, non rispondano ai livelli di professionalità richiesti o non siano di un livello qualitativo soddisfacente, il Comune invierà una prima comunicazione formale di richiamo al fornitore con l'indicazione delle carenze rilevate. A tale prima comunicazione, il fornitore deve rispondere entro 5 (cinque) giorni lavorativi indicando i comportamenti, i tecnici attivati e le soluzioni da porre in essere, entro al massimo 3 (tre) giorni lavorativi a decorrere dalla data della risposta, per risolvere le criticità e le carenze. Qualora si verificassero successivamente i medesimi problemi di qualità e/o di inadeguatezza e/o scarsa professionalità, il Comune potrà inviare una seconda comunicazione di richiamo ed applicare contestualmente una penale di 1/3.000 (un tre millesimo o 0,33‰) al giorno lavorativo per ogni episodio contestato. Al perdurare dei problemi l'Ente potrà continuare ad applicare le penali come sopra specificato.

P2 - Non rispetto dei requisiti o degli adempimenti previsti dall'art.47 del DL 77/2021; si rimanda alla lettura del capitolo precedente, capitolo 5 "ULTERIORI REQUISITI DI AS".

7. PIANO OPERATIVO DELL'AS

Il Fornitore dovrà presentare entro 15 giorni lavorativi dalla data di stipula del Contratto e pena l'applicazione delle penali di cui al CTAQ, un "*Piano Operativo*" che riporti almeno i contenuti di cui al par. 3.2.1 del CTAQ.

LUCA
BERTELLI
Comune di
Firenze
25.10.2023
09:12:10
GMT+01:00