Affidamento fornitura di un servizio di di Security Operation Center (SOC)

DISCIPLINARE E CAPITOLATO

RDO 6486637 Cig BC989DFDA0

Il presente documento di gara contiene le condizioni di fornitura integrative alla documentazione relativa alla disciplina del sistema di e-procurement "Acquisti in rete PA" – strumento MEPA.

1. PREMESSA

L'azienda sanitaria Locale Uslumbria1 intende innalzare il proprio livello di postura cyber secondo quanto previsto dalle normative vigenti e dagli standard internazionali sulla sicurezza informatica.

La crescente digitalizzazione dei servizi e dei processi aziendali ha portato a un incremento significativo delle minacce informatiche, sia in termini di numero che di sofisticazione. Attacchi mirati, campagne di malware, phishing, ransomware e attività di cybercrime organizzato rappresentano oggi un rischio concreto per la continuità operativa e la protezione dei dati sensibili.

In questo scenario, diventa fondamentale dotarsi di un sistema strutturato di **monitoraggio, rilevamento e risposta agli incidenti di sicurezza**, in grado di garantire la massima tempestività ed efficacia nella gestione delle minacce.

Il presente capitolato ha come obiettivo la selezione di un fornitore qualificato per l'erogazione di un servizio di **Security Operation Center (SOC)** esternalizzato, capace di assicurare:

- la sorveglianza continua **H24/7** delle infrastrutture informatiche
- il rilevamento e la correlazione avanzata di eventi di sicurezza utilizzando sistemi basati su intelligenza artificiale
- la gestione strutturata degli incidenti e la loro risoluzione
- la reportistica periodica e l'analisi proattiva delle vulnerabilità

- rispetto delle normative vigenti in materia di protezione dei dati personali (es. GDPR) e delle linee guida nazionali ed europee in ambito cybersecurity
- la produzione di evidenze e report a supporto delle attività di audit, certificazioni di sicurezza e conformità a standard di riferimento (es. ISO/IEC 27001, NIS2)
- Il supporto specialistico per le attività di governance, definizione delle strategie di sicurezza e adeguamento normativo
- La gestione della piattaforma Sophos Central per i prodotti
    - Intercept X Advanced con XDR
- La gestione della Piattaforma di TrendMicro Security mail Gateway

Il SOC dovrà quindi rappresentare il **punto centrale di controllo della sicurezza dell'azienda**, fornendo competenze, processi e tecnologie avanzate per incrementare il livello di resilienza dell'Ente contro le minacce cyber.

2. DESCRIZIONE DEL SERVIZIO E MODALITA' DI EROGAZIONE

Il Servizio SOC richiesto dall'azienda sanitaria Locale Uslumbria1 deve individuare e prevenire le minacce, identificare e risolvere vulnerabilità, analizzare e rispondere agli attacchi e agli incidenti di sicurezza informatica.

Il Servizio deve essere erogato in lingua italiana in modalità 24x7x365.

2.1 PERIMETRO INFRASTRUTTURA OGGETTO DEL SERVIZIO

Ad oggi l'azienda sanitaria Locale Uslumbria1 dispone di un controllo e monitoraggio ridotto per alcune log sources offerta dalla regione attraverso la società in-house Puntozero.

Il perimetro attualmente coperto è però limitato alle seguenti sorgenti:

- 14 Domani Controller
- 5 Firewall perimetrali di solo 3 delle 90 sedi dell'ente
- Console Cloud Sophos EndPoint Protection
- Piattaforma Zimbra

Oltre ad essere limitato anche nelle modalità di erogazione e risposta di eventuali incidenti

Per tanto tale perimetro va integrato con tutto il resto dei dispositivi e soluzioni presenti all'interno dell'infrastruttura informatica dell'organizzazione che dovrà essere oggetto del Servizio SOC quali:

- Postazioni di lavoro: 3500
- Server: 400 virtuali su due datacenter
- Utenti: 4500
- Firewall Watchguard su ogni sede: 80
- Caselle di posta elettronica: 5500
- Piattaforma VPN centralizzata Sonicwall: 500 utenti
- Piattaforma di Collaboration Microsoft 365
- Piattaforma antispam Trend Micro Email Security
- Piattaforma NAC (FortiNAC): 500 Switch
- Piattaforma Wifi Centralizzata Huawei: 560 AP
- Sonde IDS: 4
- Piattaforma IAM/PAM
- Piattaforma WAF (web application Firewall) per 32 servizi esposti in internet

2.2 EROGAZIONE DEL SERVIZIO SOC

L'obiettivo dell'azienda è quello di innalzare il livello di postura cyber sia a livello applicativo che infrastrutturale.

Nel dettaglio si richiede la fornitura dei seguenti servizi, che tutti insieme costituiscono il Servizio SOC.

Presidio Sicurezza piattaforma Microsoft 365

È richiesto il presidio del perimetro della piattaforma di Microsoft 365 tenendo conto dei servizi cloud, delle identità, delle applicazioni e degli endpoint locali che vi accedono. Nell'implementazione delle soluzioni tecnologiche il fornitore dovrà tenere conto delle seguenti specifiche:

- le caratteristiche delle specifiche licenze M365 presenti in azienda
- la soluzione di endpoint security presente in azienda
- l'infrastruttura firewall disponibile;
- tutte le soluzioni tecniche e prassi di sicurezza già implementate

Gestione piattaforma Sophos Central

Intercept X Advanced with XDR

Si richiede che la gestione di *Intercept X Advanced with XDR* comprenda l'installazione, la configurazione e il mantenimento delle componenti endpoint con XDR su tutti i dispositivi aziendali (Windows, macOS, server), inclusa la distribuzione dell'agent e la verifica dei requisiti di sistema. Devono essere definite e applicate policy per la *Threat Surface Reduction*, il controllo delle applicazioni, il filtering del web, il monitoraggio dei dispositivi periferici e il blocco automatico di attività sospette, come il ransomware, con rollback dei file dove previsto. È inoltre necessario configurare il sistema di rilevamento e risposta (EDR/XDR) per abilitare monitoraggio continuo, raccolta e analisi dei log, alerting, isolamento remoto dei dispositivi in caso di incidente, investigazioni forensi e reportistica regolare (alert quotidiani, settimanali e mensili). Deve essere garantita la formazione o affiancamento al personale IT per la gestione ordinaria e quella per la risposta agli incidenti, compresa la root-cause analysis.

Piattaforma VPN SonicWall

Si richiede una gestione che preveda il monitoraggio e la onfigurazione dell'architettura di accesso remoto basata su principi Zero Trust, ossia con verifiche rigorose su identità, stato dei dispositivi (device health), e policy granulare per le risorse cui accedere. Occorre configurare e monitate i gateway (on-premises o in cloud) e/o agent dove necessario, definire le regole per l'accesso alle applicazioni (sia agentless che agent-based), segmentare le risorse per minimizzare i movimenti laterali in caso di compromissione, proteggere remote desktop (es. RDP) e altri accessi critici, possibilmente integrando metodi più sicuri (autenticazione a più fattori, opzioni passwordless, etc.). Devono essere previste procedure per l'onboarding/decomissioning di utenti e dispositivi, nonché il monitoraggio degli accessi, dei log di utilizzo delle applicazioni, report sull'utilizzo, alert su accessi anomali o dispositivo non conforme, e la revisione periodica delle policy di accesso.

Gestione della piattaforma TrendMicro Email Security Gateway

Si richiede la gestione della piattaforma *TrendMicro Email Security* con l'attivazione e la supervisione dei principali servizi di protezione avanzata della posta elettronica.

La componente **Email Protection (antispam)** dovrà essere configurata per garantire il filtraggio avanzato contro spam, malware e phishing, con aggiornamento costante delle regole di blocco e tuning delle whitelist/blacklist.

È richiesta inoltre la gestione del servizio di **Incident Response**, con la capacità di rilevare e bloccare/rimuovere messaggi malevoli già recapitati nelle mailbox, applicare azioni di rimozione centralizzata e fornire reportistica post-incidente.

Vulnerability Assessment

È richiesta l'esecuzione di Vulnerability Assessment per identificare, classificare e prioritizzare le vulnerabilità dei sistemi informatici, delle reti, delle applicazioni e dei dispositivi dell'azienda sanitaria Locale Uslumbria1 . Lo scopo di questa attività non è quello di fornire soltanto l'elenco delle vulnerabilità, ma anche una valutazione del loro livello di rischio

Viene richiesto al fornitore di procedere secondo gli step di seguito descritti:

1) Raccolta delle informazioni (Asset Discovery & Inventory)
    a. Identificazione degli asset (server, endpoint, dispositivi IoT, applicazioni)
    b. Mappatura della superficie di attacco.
2) Scanning delle vulnerabilità
    a. Utilizzo di tool automatici che confrontano quanto rilevato con Database aggiornati di vulnerabilità note (es. CVE)
3) Analisi e classificazione
    a. Prioritizzazione basata sulla probabilità di sfruttamento e potenziale impatto.
4) Reportistica
    a. Report dettagliati con elenco e classificazione delle vulnerabilità
    b. Suggerimenti di remediation

Penetration Test (PT)

Si richiede l'erogazione di un servizio di **Penetration Test (PT)** in modalità **black box** su 6 (sei) **web application aziendali**, finalizzato a identificare vulnerabilità di sicurezza sfruttabili da un attaccante esterno privo di informazioni preliminari.

Per ciascuna web application sono previsti **due test all'anno**, da svolgersi a distanza di circa sei mesi l'uno dall'altro, al fine di garantire un monitoraggio costante dell'esposizione e delle eventuali nuove vulnerabilità introdotte da aggiornamenti o modifiche applicative. Le attività dovranno includere la fase di raccolta informazioni (reconnaissance), analisi delle superfici di attacco, test manuali e automatici secondo le linee guida OWASP, e l'elaborazione di un **report tecnico dettagliato** corredato da **executive summary**, **descrizione delle vulnerabilità rilevate**, **evidenze tecniche**, **valutazione del rischio**, e **raccomandazioni di**

remediation. È richiesto infine un **debriefing finale** per ogni attività di test, con possibilità di confronto tecnico con il team interno per la validazione delle evidenze e il supporto alla pianificazione delle azioni correttive.

Web Application Firewall (WAF)

Il servizio SOC fornito deve includere anche la gestione e il monitoraggio della piattaforma WAF per la protezione delle applicazioni web dell'azienda da attacchi che sfruttano vulnerabilità a livello applicativo.

Il WAF attualmente in esercizio garantisce le seguenti funzionalità minime:

- Protezione da attacchi DoS e DDoS
- Protezione da attacchi comuni OWASP Top 10**,** inclusi:
    - SQL Injection (SQLi)
    - Cross-Site Scripting (XSS)
    - File Inclusion (LFI/RFI)
    - Command Injection e Remote Code Execution (RCE)
    - Cross-Site Request Forgery (CSRF)
- Ispezione del traffico HTTP/HTTPS con capacità di analisi su header, cookie, parametri URL, body di richieste e risposte.
- Modalità operative configurabili: whitelist, blacklist, learning mode.
- Aggiornamento continuo delle regole di sicurezza tramite feed di threat intelligence.

Cyber Threat Intelligence

Il Fornitore dovrà garantire l'erogazione di servizi di **Threat Intelligence** con particolare riferimento alla componente di **Identity Intelligence**, al fine di monitorare e prevenire i rischi derivanti dall'esposizione non autorizzata di credenziali aziendali.

In particolare, il servizio dovrà prevedere:

- il monitoraggio continuativo di fonti open, deep e dark web, nonché di repository e marketplace noti per la diffusione illecita di credenziali;

- l'individuazione di credenziali (username, password, token, API key) esposte o compromesse, con riferimento esclusivo al dominio di posta elettronica **@uslumbria1.it**;
- la generazione di alert tempestivi in caso di rilevamento di credenziali correlate al dominio, con evidenza della fonte e del contesto di esposizione;
- la produzione di report periodici sul livello di rischio e sull'andamento delle esposizioni rilevate;
- la fornitura di raccomandazioni operative per la mitigazione del rischio e la gestione sicura delle identità compromesse.

Il servizio dovrà integrarsi con i processi di Incident Response del SOC, consentendo una gestione strutturata degli eventi di compromissione delle identità digitali.

Monitoraggio continuo e gestione dei log

Si richiede l'implementazione di soluzioni tecniche per l'analisi continuativa del perimetro di sicurezza informatica quali SIEM (Security Information Enterprise Management), SOAR (Security Orchestration, Automation, and Response) o XDR (funzionalità di rilevamento e reazione estese), allo scopo di monitorare l'ambiente applicativo locale, i sistemi cloud, le applicazioni, le reti e i dispositivi e scoprire anomalie o comportamenti sospetti.

Il fornitore dovrà predisporre le infrastrutture necessarie per la raccolta, la manutenzione e l'analisi dei dati di log prodotti dalle applicazioni cloud ovvero da ogni endpoint, sistema operativo, applicazione locale ed evento di rete parte dell'ecosistema dell'istituto e dovrà provvedere al continuo miglioramento e allo sviluppo delle regole di correlazione delle informazioni raccolte e di riconoscimento degli eventi di sicurezza informatica.

Il fornitore dovrà periodicamente consegnare la documentazione relativa alle tendenze degli eventi analizzati contenente tutte le informazioni raccolte e analizzate durante uno specifico arco temporale con lo scopo di andare a definire il trend di eventi analizzati e segnalati.

Tutte le applicazioni, gli strumenti di sicurezza e i processi utilizzati dal fornitore dovranno essere conformi alle normative sulla privacy.

Rilevamento degli eventi, analisi e segnalazione

Il fornitore dovrà identificare le minacce provenienti dalle varie fonti, filtrando i falsi positivi dai problemi reali, classificando le minacce in base alla gravità, all'urgenza e al potenziale impatto sull'azienda. Le segnalazioni utili ai fini di investigazione in materia di sicurezza

possono essere originate ed inviate al SOC anche dai referenti dell'Istituto che dovessero rilevare anomalie.

Il SOC dovrà supportare i referenti INMI nella predisposizione delle segnalazioni utili ai fini di investigazione in materia di sicurezza alle autorità competenti (CSIRT Italia istituito presso l'Agenzia per la Cybersicurezza Nazionale (ACN), Garante per la Protezione dei Dati Personali, ecc.).

Incident Response

Deve essere inclusa nel servizio la risposta agli incidenti informatici preferibilmente basata su pratiche di settore e tassonomia ACN. Il fornitore potrà utilizzare playbook predefiniti per automatizzare le risposte agli incidenti di sicurezza e ridurre i tempi di risposta.

A seguito dell'analisi dell'eventuale incidente il fornitore individuerà un'attività di risposta o una contromisura. Le misure da adottare possono comprendere l'arresto o l'isolamento degli endpoint e delle applicazioni interessate, la sospensione degli account compromessi, la rimozione dei file infetti e l'esecuzione di software antivirus e anti-malware, attività che il SOC potrà svolgere in autonomia ovvero in collaborazione con altri fornitori indicati dall'Istituto. Le policy di intervento verranno stabilite in fase di contrattualizzazione del Servizio.

Ripristino e correzione

In seguito ad un attacco il fornitore contribuirà al ripristino dello stato originale dell'azienda dando indicazioni all'Istituto o a suoi fornitori terzi in merito alle attività da effettuarsi sulle applicazioni ovvero sui sistemi interessati.

Perfezionamento della sicurezza

A seguito di un incidente il fornitore dovrà svolgere indagini per identificare le vulnerabilità, i processi di sicurezza insufficienti e altri elementi che hanno contribuito all'incidente.

Nell'ambito di tale attività il fornitore dovrà predisporre un Report Tecnico contenente il dettaglio di tutte quelle azioni che dovranno essere intraprese dall'Istituto (Interventi reattivi, aggiornamenti delle politiche di sicurezza, misure preventive da adottare per la gestione degli incidenti) con lo scopo di fornire informazioni utili per rafforzare le misure di sicurezza.

2.3 TEMPISTICHE

Il Servizio dovrà essere attivato entro e non oltre 45 giorni solari dalla data di sottoscrizione del contratto.

La durata del contratto sarà di 12 mesi a decorrere dalla data di sottoscrizione, senza possibilità di tacito rinnovo.

3. LIVELLI DI SERVIZIO

Il presenta capitolo descrive i livelli di qualità minimi attesi per il Servizio SOC.

Il fornitore dovrà misurare i suddetti livelli di servizio mentre sarà a carico dell'la verifica del rispetto degli stessi.

INDICATORE	GRAVITA'	SLA	PENALE
Tempo di presa in carico degli eventi relativi a incidenti di sicurezza informatica.	P1	<30 minuti, dalla data/ora di segnalazione dell'evento.	0,1% canone annuo per ogni h lavorativa di ritardo.
	P2	<60 minuti, dalla data/ora di segnalazione dell'evento.	0,05% canone annuo per ogni h lavorativa di ritardo.
	P3	<2h , dalla data/ora di segnalazione dell'evento	0,085% canone annuo per ogni h lavorativa di ritardo.
	P4	<4h, dalla data/ora di segnalazione dell'evento	0,025% canone annuo per ogni gg lavorativo di ritardo.
Tempo di avvio della fase di mitigazione degli eventi relativi a incidenti di sicurezza informatica.	P1	1 ora, dalla data/ora di segnalazione dell'evento.	0,2% canone annuo per ogni h lavorativa di ritardo.
	P2	2 ore, dalla data/ora di segnalazione dell'evento.	0,1% canone annuo per ogni h lavorativa di ritardo.
	P3	3 ore, dalla data/ora di segnalazione dell'evento.	0,75% canone annuo per ogni h lavorativa di ritardo
	P4	4 ore, dalla data/ora di segnalazione dell'evento	0,05% canone annuo per ogni gg lavorativo di ritardo.

P1 CRITICO – Impatto con interruzione totale di un servizio core o compromissione dell'intera infrastruttura aziendale (es. attacco ransomware esteso o violazione massiva di dati sensibili). Richiede un intervento immediato del team di Incident Response H24 per ripristinare le attività vitali.

P2 ALTO – Impatto significativo su servizi importanti ma non completamente bloccanti, oppure isolato a un intero dipartimento o sede periferica. La continuità operativa è parzialmente degradata e il workaround non è disponibile o è poco sostenibile nel medio periodo.

P3 MEDIO – Impatto moderato che riduce le prestazioni di un'applicazione o coinvolge un numero limitato di utenti senza interrompere i flussi di lavoro principali. Esiste un workaround temporaneo o il problema influisce su funzionalità non critiche per il business.

P2 BASSO – Impatto minimo o nullo sulle operazioni quotidiane, spesso riconducibile a anomalie estetiche, richieste di informazioni o falsi positivi. Viene gestito come attività ordinaria pianificabile, senza richiedere l'attivazione delle procedure di emergenza.

L'importo dovuto a titolo di penale è compensato con quanto dovuto per pagamenti dall'Istituto alla data di applicazione della penale.

Qualora l'ammontare delle penali maturate superi il 10% dell'importo contrattuale, l'Istituto si riserva la facoltà di risolvere il contratto.

4. REQUISITI TECNICI E ORGANIZZATIVI

Il Servizio SOC sarà erogato attraverso un team di lavoro sotto la responsabilità e l'organizzazione del Fornitore.

Il team sarà oggetto di valutazione da parte dell'Istituto in termini di:

- titolo di studio in discipline coerenti con l'oggetto del Servizio;
- anzianità professionale;
- esperienze lavorative aventi ad oggetto ambiti coerenti con le attività di cui al presente capitolato. Sarà pertanto valutata l'esperienza nella pianificazione, realizzazione e monitoraggio di progetti IT nel campo della cyber security nonché l'esperienza in metodologie di security governance e management, tecniche di problem solving e risk management e metodologie di vulnerability assessment, penetration test, compliance management e security audit;
- ottenimento di certificazioni quali ad esempio CompTIA Security+,CompTIA CySa+, CEH, OSCP, GCIH e altre (le certificazioni dovranno essere mantenute aggiornate e in corso di validità per tutta la durata contrattuale).

5. PROSPETTO ECONOMICO

DESCRIZIONE	QTA'	TOTALE
Servizi SOC come da capitolato – canone annuale	1	100.000€
Opzione rinnovo di 12 mesi ai sensi dell'art. 120, comma 10 del D.lgs. 36/2023	1	100.000€
		200.000€

Modalità di esercizio dell'opzione

L'opzione di rinnovo è una facoltà esclusiva della Stazione Appaltante e non costituisce alcun diritto in capo all'aggiudicatario. L'eventuale attivazione sarà subordinata alla permanenza dell'interesse pubblico, alla disponibilità di bilancio e alla valutazione positiva del servizio reso. La Stazione Appaltante comunicherà l'intenzione di avvalersi del rinnovo mediante formale comunicazione via PECL'operatore economico aggiudicatario è obbligato ad eseguire le prestazioni oggetto del rinnovo.

VALORE DEL CONTRATTO

L'importo complessivo presunto per l'intera durata dell'appalto, soggetto a ribasso, è indicato nell'apposita maschera del sistema di e-procurement "Acquisti in rete PA" – strumento MEPA. Il suddetto importo, calcolato ai sensi dell'art. 14 comma 4 del D. Lgs. 36/2023, comprende:

- i costi della manodopera e gli oneri aziendali per l'adempimento delle disposizioni in materia di salute e sicurezza sui luoghi di lavoro. Nell'offerta economica l'operatore indica, a pena di esclusione, i predetti costi eccetto che nelle forniture senza posa in opera e nei servizi di natura intellettuale *(art.108 c.9 del D. Lgs. 36/2023);*
- i costi di sicurezza di natura interferenziale che ammontano complessivamente ad € 0,00 (IVA esclusa) per tutta la durata dell'appalto trattandosi di fornitura di beni senza messa in opera;
- i costi, espressi e non, derivanti per adempiere a tutto quanto richiesto dal servizio oggetto dall'appalto e necessari per assicurare la perfetta esecuzione del servizio;

Non sono ammesse offerte in aumento, parziali o condizionate, rispetto alla base d'asta indicata.

6. TEMPI DI CONSEGNA E DURATA

Il servizio di Security Operation Center (SOC) dovrà essere operativo come richiesto dalla normativa NIS2 entro il 31/10/2026. La durata del servizio è di 12 mesi.

7. TIPOLOGIA DI PROCEDURA E CRITERI DI SELEZIONE DEL CONTRAENTE

- Tipologia di procedura: procedura negoziata senza bando *(ai sensi dell'art.50 comma e) del Dlgs 36/2023 con almeno 5 operatori*.
- Criteri di aggiudicazione: prezzo più basso *ai sensi dell'art. 50 c. 4 del Dlgs 36/2023*
- Esclusione automatica delle offerte (*art.54 del Dlgs 36/2023*): non applicabile per la procedura in questione in quanto trattasi di servizi.
- Ai sensi dell'art. 107 comma 3 del Dlgs 36/2023 e parere MIT n. 2615 18/07/2024 la stazione appaltante ha stabilito di ricorrere all'inversione procedimentale. Con l'inversione procedimentale, si procede preliminarmente alla valutazione dell'offerta economica, ed infine alla verifica della documentazione amministrativa del miglior offerente verificando il possesso dei requisiti di ordine generale accedendo al fascicolo virtuale dell'operatore economico FVOE.

La stazione appaltante si riserva di non procedere all'aggiudicazione se nessuna offerta risulti conveniente o idonea in relazione all'oggetto del contratto *(ai sensi dell'art.108 c.10 del DLgs 36/2023)*.

8. DOCUMENTAZIONE AMMINISTRATIVA

L'operatore economico dovrà produrre la seguente documentazione amministrativa:

1. DGUE- utilizzare il modello messo a disposizione dalla S.A.– debitamente compilato e firmato digitalmente dal Legale rappresentante della Ditta concorrente
2. Dichiarazioni sulla tracciabilità dei flussi finanziari, come da modello allegato, ai sensi della L.136/2010

STIPULA DEL CONTRATTO

La conclusione del contratto avverrà, *ai sensi e per gli effetti dell'art.18 comma 1 del D.lgs. n. 36/2023,* all'interno del sistema MEPA.

Il fornitore, al momento della stipula è tenuto a

1. Assolvere per contratti di importo uguale o superiore a €40.000,00, *ai sensi dell'art.18 c.10 del Dlgs 36/2023*, **all'imposta di bollo secondo** la tabella indicata nell'Allegato I.4 del Dlgs 36/2023, dandone poi riscontro con **l'invio della ricevuta all'indirizzo PEC** **aslumbria1@postacert.umbria.it**.

Il pagamento della suddetta imposta pari ad € 40,00 potrà essere effettuato unicamente per via telematica, utilizzando il modello "F24 Versamenti con elementi identificativi" (F24 ELIDE).

Il modello di versamento deve contenere:

- l'indicazione dei codici fiscali delle parti (stazione appaltante/ente concedente e appaltatore); il Codice Identificativo di Gara (CIG) o, in sua mancanza, un altro identificativo univoco del contratto.

Per la compilazione del modello "F24 ELIDE" dovranno essere utilizzati i seguenti codici tributo:

- ✓ 1573 denominato Imposta di bollo sui contratti;
- ✓ 1574 denominato Imposta di bollo sui contratti – SANZIONE;
- ✓ 1575 denominato Imposta di bollo sui contratti – INTERESSI;
- ✓ 40 denominato stazione appaltante. Questo codice permette di identificare il soggetto controparte del contratto.

I codici tributo sopra citati devono essere esposti in corrispondenza delle somme indicate nella colonna "*importi a debito versati*", secondo le seguenti modalità.

Nella sezione "***Contribuente***" devono essere indicati:

- ✓ nei campi "*codice fiscale*" e "*dati anagrafici*", il codice fiscale e i dati anagrafici del soggetto tenuto al versamento;

- ✓ nel campo "*Codice fiscale del coobbligato, erede, genitore, tutore o curatore fallimentare*", il codice fiscale della stazione appaltante, unitamente al codice identificativo "40", da indicare nel campo "*codice identificativo*".

Nella sezione "***Erario ed altro***":

- ✓ nel campo "*tipo*", la lettera "R";□ nel campo "*elementi identificativi*", il codice identificativo di gara (CIG), o altro codice indicato dalla stazione appaltante, del contratto per il quale si versa l'imposta di bollo;
- ✓ nel campo "*codice*", uno dei codici tributo;
- ✓ nel campo "*anno di riferimento*", l'anno di stipula del contratto, nel formato "AAAA";
- ✓ nei campi "*codice ufficio*" e "*codice atto*", nessun valore.

FATTURAZIONE E PAGAMENTO

L'emissione della fattura sarà emessa quadrimestralmente e solo successivamente alla verifica del corretto svolgimento del servizio accertato tramite SAL (Stato avanzamento lavori).

La liquidazione delle fatture avverrà entro 60gg dal ricevimento della fattura, previo:

- esito positivo della verifica di conformità, diretta a certificare che le prestazioni contrattuali siano state eseguite a regola d'arte sotto il profilo tecnico e funzionale, in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni del contratto, nonché nel rispetto delle vigenti normative e delle eventuali leggi di settore;
- esito positivo della verifica contabile, diretta a verificare che gli importi fatturati siano rispondenti alle prestazioni erogate;
- esito positivo della verifica di regolarità contributiva (DURC) dell'appaltatore, dei subappaltatori e delle imprese ausiliarie;
- *(in caso di subappalto)* certificazione dell'avvenuto pagamento di quanto dovuto dall'Appaltatore al subappaltatore (anche secondo le disposizioni della tracciabilità dei flussi finanziari di cui alla Legge 136/2010); resta ferma quanto previsto dall'art.119 del D.Lgs n.36/2023;
- *(in caso di avvalimento)* certificazione dell'avvenuto pagamento di quanto dovuto dall'Appaltatore all'impresa ausiliaria secondo quanto previsto dal relativo contratto di avvalimento;

- rispetto di ulteriori eventuali obblighi normativi.

L'Azienda, in fase di liquidazione delle prestazioni contrattuali, opererà le ritenute obbligatorie per legge sull'importo netto delle prestazioni secondo quanto previsto dalle normative vigenti o che entreranno in vigore durante l'esecuzione del contratto.

Le fatture dovranno contenere le seguenti informazioni:

- "Tripletta" (art.3 del DM 7.12.2018):
  - Numero di Ordine NSO (esempio 0500XXXXX/A0A/001): campo <DatiOrdineAcquisto> <IdDocumento>
  - codice univoco di fatturazione: UF9FAJ campo <DatiOrdineAcquisto> <CodiceCommessaConvenzione>;
  - data ordine: campo <DatiOrdineAcquisto> <Data>;
- Codice CIG (campo <DatiOrdineAcquisto><CodiceCIG>);
- PIVA Committente: 03301860544;
- Codice Fiscale Committente: 03301860544;
- Applicazione della scissione dei pagamenti ai sensi dell'art. 17- ter del D.P.R. n. 633/1972 (c.d. split payment);
- Descrizione della prestazione eseguita, imponibile e IVA.

La Stazione Appaltante si riserva la possibilità di accogliere modifiche alle modalità di fatturazione proposte dall'Appaltatore.

PENALI

In caso di riscontrata irregolarità nell'esecuzione del servizio o di mancato rispetto delle disposizioni contenute nel presente capitolato di appalto e nelle eventuali parti integrative e migliorative contenute nell'Offerta Tecnica, l'Appaltatore è tenuto al pagamento di una penale calcolata in rapporto alla gravità dell'inadempienza e alla recidiva fatta salva la risoluzione del contratto.

Le penalità saranno precedute da regolare contestazione dell'inadempienza. L'appaltatore è tenuto a fornire giustificazioni scritte e documentate, se richieste dall'Azienda, in relazione alle contestazioni mosse. Se entro il termine previsto dall'Azienda, di massimo 5 gg –termine

ridotto in casi di urgenza in base al caso specifico-, l'Appaltatore non produce alcuna comprovata giustificazione, l'Azienda applicherà le penali previste dal presente capitolato.

In caso di recidiva nell'arco di 30 giorni, la penalità già applicata potrà essere aumentata fino al raddoppio.

Le penali non si applicano nel caso in cui l'inesatto o mancato adempimento dell'Appaltatore sia determinato da cause di forza maggiore o impossibilità sopravvenuta alla stessa non addebitabili. Gli inadempimenti che l'Appaltatore ritiene ascrivibili a tali eventi devono essere segnalati, per iscritto, all'Azienda entro 3 giorni lavorativi dall'inizio del loro avverarsi sotto pena di decadenza dal diritto al risarcimento.

In ogni caso per forza maggiore si intende ogni situazione o evento imprevedibile ed eccezionale, indipendente dalla volontà delle parti e non attribuibile ad una loro colpa o negligenza, che impedisca ad una delle parti di adempiere ad uno degli obblighi derivanti dal contratto, senza possibilità di ovviare a tale impedimento nonostante tutta la diligenza dispiegata. Se una delle parti si trova in caso di forza maggiore, ne avvisa senza indugio e nel più breve tempo possibile l'altra parte, precisando la natura, la durata possibile e gli effetti prevedibili di tale avvenimento.

Per gli inadempimenti di seguito elencati, l'Azienda potrà applicare, anche in maniera additiva, le seguenti penali:

1- **Euro 200,00:**

per ogni giorno di ritardo rispetto ai tempi indicati nel paragrafo "Tempi di consegna";

2- **Variabile:**

per ciascuna violazione di norme contenute nel presente documento o nell'offerta dell'Appaltatore e non espressamente previste nelle penalità di cui sopra, l'Azienda si riserva l'applicazione di una penale di un valore compreso tra euro 100,00 e euro 1.000,00 per ogni inadempienza. L'entità della penale è definita a discrezione dell'Azienda, in rapporto alla gravità dell'inadempimento.

L'imposizione delle penali non impedisce l'applicazione delle norme di risoluzione contrattuale.

L'Azienda potrà compensare i crediti derivanti dall'applicazione delle penali di cui al presente articolo con quanto dovuto al fornitore a qualsiasi titolo ovvero in difetto avvalersi della cauzione senza bisogno di diffida ulteriore, accertamento o procedimento giudiziario.

La richiesta e/o il pagamento delle penali di cui al presente articolo non esonera in nessun caso l'Appaltatore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

L'Appaltatore prende atto che l'applicazione delle penali previste dal presente articolo non preclude il diritto dell'Azienda a richiedere il risarcimento degli eventuali maggior danni.

In caso d'inadempienza dell'Appaltatore, resta ferma la facoltà dell'Azienda di ricorrere a terzi per l'esecuzione dei servizi di cui al presente capitolato addebitando all'Appaltatore i relativi costi sostenuti maggiorati del 25%.

RISOLUZIONE DEL CONTRATTO PER INADEMPIMENTO E CLAUSOLA RISOLUTIVA ESPRESSA

Le parti convengono che, oltre a quanto è genericamente previsto dall'art. 1453 del Codice Civile per i casi di inadempimento alle obbligazioni contrattuali, costituiscono motivo di risoluzione del contratto per inadempimento, e quindi la presente costituisce clausola risolutiva espressa ai sensi dell'art. 1456 del Codice Civile, le seguenti fattispecie:

a) apertura di fallimento o altra procedura concorsuale a carico dell'Appaltatore o a carico della ditta capogruppo in caso di raggruppamento di imprese;

b) messa in liquidazione, cessione illegittima del contratto o ogni diversa ipotesi di cessazione dell'attività dell'Appaltatore;

c) in caso di non rispetto della normativa in materia di subappalto;

d) mancato utilizzo del bonifico bancario o postale ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni (ai sensi dell'art.3 c. 9bis della L.136/2010);

e) violazione delle norme di sicurezza e prevenzione;

f) mancata stipulazione o rinnovo delle polizze assicurative previste dal presente documento (ove previste);

g) aver accumulato, nel corso del contratto, penali per un importo pari o superiore alla misura massima del 10% del valore del contratto;

h) impossibilità per qualsiasi motivo a tenere fede ai propri impegni contrattuali;

i) in ogni altro caso previsto dalla normativa vigente.

In tali ipotesi, il contratto potrà essere risolto di diritto, senza obbligo di costituzione in mora, con effetto immediato a seguito di comunicazione formale dell'Azienda di volersi avvalere della clausola risolutiva espressa.

Qualora si verifichi la risoluzione contrattuale per i motivi sopra indicati o per altri gravi motivi da imputarsi all'Appaltatore o il recesso anticipato rispetto alla durata del contratto, l'Azienda provvederà non solo all'incameramento della cauzione ma anche al trasferimento di proprietà dei beni senza che l'Appaltatore abbia nulla a pretendere, fatto comunque salvo il diritto al risarcimento dei danni procurati all'Azienda tra cui l'addebito delle maggiori spese derivanti per l'assegnazione del servizio ad altro operatore economico.

Sono fatte salve in favore della stazione appaltante le ipotesi di revoca o recesso ai sensi degli articoli 21 quienquies *(Revoca del provvedimento)* e 21 sexies *(Recesso dai contratti)* della legge n. 241 del 1990 e successive modificazioni e integrazioni.

NORME DI RIFERIMENTO

Per quanto non sia specificatamente contenuto nel presente Capitolato si fa espresso riferimento alle vigenti disposizioni legislative ed in particolare:

- Decreto Legislativo 36/2023;
- Delibera Direttore Generale n.913/2016 "*Approvazione del Regolamento per la disciplina transitoria di alcune fasi e procedure relative all'acquisizione di beni, servizi e lavori, in attuazione del Codice dei contratti pubblici di cui al D.Lgs. 50/2016*";
- Legge 06.07.2012, n. 94 e Legge 7.08.2012 n.135 e sim
- Tutela della salute e della sicurezza nei luoghi di lavoro (D.Lgs. 81/08);
- Codice Civile e Codice Penale;
- Altra normativa comunitaria, nazionale, regionale e regolamentare disciplinante l'esecuzione del servizio oggetto del presente appalto vigente e successiva alla data di inizio di esecuzione del presente appalto

Per quanto non previsto nel presente documento, si rinvia alla documentazione relativa alla disciplina del Mercato Elettronico, ivi compresi il Bando di Abilitazione e i relativi Allegati (es. Capitolato Tecnico, Condizioni Generali di contratto, le regole ECC) nonché in generale tutti gli atti e i documenti che disciplinano l'abilitazione, la registrazione, l'accesso e la partecipazione dei soggetti al Mercato Elettronico.

FORO COMPETENTE

Per eventuali controversie giudiziarie di qualsiasi natura, il foro competente è quello di Perugia. E'escluso il ricorso all'arbitrato.

TUTELA DEI DATI PERSONALI

I dati personali conferiti ai fini della partecipazione alla gara dai concorrenti saranno raccolti e trattati ai fini del procedimento di gara e dell'eventuale e successiva stipula e gestione del contratto secondo le modalità e le finalità di cui al GDPR 679/2016 e potranno essere comunicati:

- al personale interno dell'Azienda coinvolto nelle attività inerenti il procedimento di gara;
- ai concorrenti che partecipano alla gara e ad ogni altro soggetto che vi abbia interesse, ai sensi della legge n. 241/1990 e art.53 del D.Lgs. 50/2016;
- ad altro soggetto della Pubblica Amministrazione.

INFORMAZIONI

Informazioni e chiarimenti possono essere richiesti in via telematica con le modalità offerte dal sistema di e-procurement "Acquisti in rete PA" – strumento MEPA.

U.O.C. SISTEMI INFORMATIVI E CONTROLLO DI GESTIONE

Via Pian della Genna, 2/B - 06128 Perugia

Tel. 075-541.2299-2191

PEC: aslumbria1@postacert.umbria.it

ALLEGATO A "NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI "

Di seguito l'AZIENDA USL UMBRIA 1 viene indicata come "Azienda" ed il Fornitore viene indicato come "Fornitore/Responsabile".

DISPOSIZIONI A CARATTERE GENERALE

1. Con la sottoscrizione del presente documento il Fornitore accetta la nomina a Responsabile del trattamento (di seguito *Responsabile*) ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche *"Regolamento UE"*), per tutta la durata del contratto. A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto del Titolare, le sole operazioni di trattamento necessarie per fornire il servizio oggetto del presente contratto, nei limiti delle finalità ivi specificate, nel rispetto del Codice Privacy, del Regolamento UE e delle istruzioni nel seguito fornite;
2. I trattamenti consistono in attività di lettura, verifica, copia, analisi dei dati personali degli utenti e dei dipendenti per le finalità di assistenza e manutenzione del sistema in oggetto, così come descritto nelle allegate condizioni di fornitura, al fine di garantire la sicurezza, l'integrità e la disponibilità dei dati trattati e supportare l'Azienda in tutte le attività previste nelle condizioni contrattuali mantenendo il sistema in perfetta efficienza;
3. Trattandosi di dati inseriti nel documentale aziendale possono essere trattati in ragione delle attività oggetto del contratto i seguenti tipi di dati: i) dati comuni (anagrafici, di contatto, ecc…); ii) dati sensibili (dati sanitari/clinici);
4. Le categorie di interessati sono pazienti, utenti e dipendenti dell'Azienda Usl.
5. Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:
   a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;
   b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
   c) trattare i dati conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del trattamento;
   d) garantire la riservatezza dei dati personali trattati e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:
      - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
      - ricevano la formazione necessaria in materia di protezione dei dati personali;

- trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;

e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);

f) valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

g) su eventuale richiesta del Titolare, assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;

h) ai sensi dell'art. 30 del Regolamento UE, e nei limiti di quanto esso prescrive tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 31 a 36 del Regolamento UE;

OBBLIGHI DI PROTEZIONE DEI DATI

6. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio e il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre:
   - la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
   - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
   - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
7. In via generale, il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati in esecuzione del presente contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento- anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati.

SUB- RESPONSABILE

8. Il Responsabile del trattamento può avvalersi di subappaltatori o subcontraenti (di seguito "sub-Responsabili del trattamento") per delegargli attività specifiche del Contratto che comportano il trattamento di dati personali solo previa richiesta scritta di autorizzazione da parte del Titolare del trattamento. Nella richiesta di autorizzazione andranno specificate le attività di trattamento delegate, i dati identificativi del sub-Responsabile del trattamento e i dati del contratto di esternalizzazione.
9. Nel caso si ricorra a subappaltatori o a subcontraenti, il Fornitore/ Responsabile è obbligato a nominare con specifico

contratto o atto di nomina tali operatori quali sub-Responsabili del trattamento ai sensi dell'art 28 del Regolamento UE sulla base delle specifiche indicate al Titolare. In particolare, il sub-Responsabile del trattamento deve rispettare gli stessi obblighi a quelli forniti dal Titolare al Responsabile del trattamento con il presente documento.
Spetta al Responsabile del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti.

L'Azienda potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi che avverranno con le medesime modalità di cui ai successivi punti 19 e 20. Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Azienda diffiderà il Responsabile a far adottare al sub-Responsabile del trattamento tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, l'Azienda potrà risolvere il contratto con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

10. Il Responsabile Iniziale del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno di reputazione) in relazione anche ad una sola violazione della normativa in materia di Trattamento dei Dati Personali e/o del Contratto (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o sub-fornitori;

ESERCIZIO DEI DIRITTI DELL'INTERESSATO

11. Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. da 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti;

SUPPORTO IN CASO DI VIOLAZIONE DEI DATI PERSONALI, DATA BREACH E/O VERIFICHE DA PARTE DEL GARANTE

12. Il Responsabile dovrà collaborare con il Titolare per eseguire la valutazione d'impatto sulla protezione dei dati (art 35 del Regolamento) e la messa in atto delle misure idonee alla mitigazione del rischio;
13. Ai sensi dell'art 33 del regolamento, il Responsabile deve informare tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di qualsiasi violazione di dati personali (cd. *data breach*). La comunicazione dovrà essere accompagnata da ogni documentazione utile per permettere al Titolare di valutare la natura della violazione, la categoria dei dati e le probabili conseguenze e consentire l'adozione delle misure necessarie alla risoluzione delle cause che hanno provocato la violazione del dato.
Il Responsabile è tenuto ad affiancare il Titolare in tutte le fasi gestione del data breach da quelle iniziali di indagine e verifica fino all'adozione delle misure volte alla mitigazione del rischio. Dovrà supportare il titolare anche nelle comunicazioni agli interessati ai sensi dell'art 34 del regolamento;

14. Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare nel caso in cui riceva richieste di informazioni e di documentazione o di ispezioni da parte dell'Autorità Garante per la protezione dei

dati personali. Dovrà, inoltre, assistere il Titolare nel caso di richieste formulate dall'Autorità Garante al Titolare stesso;

DESIGNAZIONE RESPONSABILE DELLA PROTEZIONE DEI DATI

15. Il Responsabile esterno del trattamento deve comunicare al Titolare il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare;

AMMINISTRATORI DI SISTEMA

16. Il Responsabile si impegna ad attuare quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i. recante *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema".*
In particolare, dovrà procedere alla designazione formale degli amministratori di sistema nella quale dovranno essere elencati in modo analitico gli ambiti di operatività consentiti in base al profilo autorizzato.

    Sarà inoltre tenuto ad effettuare una verifica del loro operato con cadenza almeno annuale in modo da controllare il rispetto di tutte le misure di organizzative, tecniche e di sicurezza riguardo al trattamento dei dati personali;

LOCALIZZAZIONE DEI DATI

17. Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare;

VERIFICHE DA PARTE DEL TITOLARE

18. Sarà obbligo del Titolare del trattamento vigilare per tutta la durata del contratto, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento da parte del Responsabile, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento;
19. Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione- verifiche periodiche o circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso.
    Nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Azienda diffiderà il Fornitore ad adottare tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato;

20. Nel caso in cui il Fornitore agisca in modo difforme o contrario alle legittime istruzioni del Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento risponde del danno causato agli "interessati" e/o non si sia adeguato a seguito di diffida, l'Azienda potrà risolvere il contratto, salvo il risarcimento del maggior danno;

ADEGUAMENTI ALLA NORMATIVA

21. Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.
22. Durante l'esecuzione del Contratto, qualora la normativa lo richieda, il responsabile dovrà adottare un codice di condotta approvato o un meccanismo di certificazione così come specificato agli articoli 40 e 42 del Regolamento

LEGALE RAPPRESENTANTE

(Firmato digitalmente per accettazione)

ALLEGATO B "PATTO DI INTEGRITA' "

Questo patto d'integrità stabilisce la reciproca, formale obbligazione dell'Azienda USL Umbria 1 e l'operatore economico di conformare i propri comportamenti ai principi di lealtà, trasparenza e correttezza nonché l'espresso impegno anti-corruzione di non offrire, accettare o richiedere somme di denaro o qualsiasi altra ricompensa, vantaggio o beneficio, sia direttamente che indirettamente tramite intermediari, al fine dell'assegnazione del contratto e/o al fine di distorcerne la relativa corretta esecuzione.

Il personale, i collaboratori ed i consulenti dell'Azienda USL Umbria 1 impiegati ad ogni livello nell'espletamento della gara e nel controllo dell'esecuzione del contratto in oggetto, sono consapevoli del presente Patto d'Integrità, il cui spirito condividono pienamente, nonché delle sanzioni previste a loro carico in caso di mancato rispetto del presente Patto.

Il sottoscritto Operatore economico si impegna a segnalare all'Azienda USL Umbria 1 qualsiasi tentativo di turbativa, irregolarità o distorsione nella fase di esecuzione del contratto, da parte di ogni interessato o addetto o di chiunque possa influenzare le decisioni relative all'affidamento in oggetto.

Il sottoscritto operatore economico dichiara di non trovarsi in situazioni di controllo o di collegamento (formale e/o sostanziale) con altri concorrenti e che non si è accordato e non si accorderà con altri partecipanti alla gara.

Il sottoscritto Operatore economico si impegna a non conferire incarichi di collaborazione al personale dipendente di questa Azienda USL coinvolto nell'appalto, od ai loro familiari, ivi compresi gli affini entro il secondo grado, durante la fase di esecuzione del contratto e nei tre anni successivi alla conclusione del contratto stesso.

I dipendenti che, negli ultimi tre anni di servizio, hanno esercitato poteri autoritativi o negoziali per conto dell'Azienda USL non possono svolgere, nei tre anni successivi alla cessazione del rapporto di pubblico impiego, attività lavorativa o professionale presso i soggetti privati destinatari dell'attività della stessa Azienda USL svolta attraverso i medesimi poteri. I contratti conclusi e gli incarichi conferiti in violazione di quanto previsto dal presente comma sono nulli ed è fatto divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni con obbligo di restituzione dei compensi eventualmente percepiti e accertati ad essi riferiti.

Il sottoscritto Operatore economico prende nota e accetta che nel caso di mancato rispetto degli impegni assunti con il presente Patto di Integrità comunque accertato dall'Amministrazione, potranno essere applicate le seguenti sanzioni:

- risoluzione o perdita del contratto;
- escussione della cauzione di validità dell'offerta;
- escussione della cauzione di buona esecuzione del contratto;
- responsabilità per danno arrecato all'Azienda USL Umbria 1 nella misura dell'8% del valore del contratto, impregiudicata la prova dell'esistenza di un danno maggiore;
- responsabilità per danno arrecato agli altri concorrenti della gara nella misura dell'1% del valore del contratto per ogni partecipante, sempre impregiudicata la prova predetta;
- esclusione del concorrente dalle gare d'appalto indette dall'Azienda USL Umbria 1 per 5 anni.

Il presente Patto di Integrità e le relative sanzioni applicabili resteranno in vigore sino alla completa esecuzione del contratto in oggetto.

Ogni controversia relativa all'interpretazione, ed esecuzione del presente patto d'integrità fra Azienda USL Umbria 1 ed i concorrenti e tra gli stessi concorrenti sarà risolta dall' Autorità Giudiziaria competente.

LEGALE RAPPRESENTANTE

(Firmato digitalmente per accettazione)

ALLEGATO C "DISCIPLINARE TECNICO PER L'INTEGRAZIONE DI SISTEMI CON L'INFRASTRUTTURA IT DELL'AZIENDA USL UMBRIA 1 "

Art. 1.C. SCOPO

La presente procedura definisce le specifiche e le regole che i sistemi installati da ditte/fornitori esterni dovranno rispettare relativamente agli aspetti inerenti l'infrastruttura IT (Information Technology).

Art 2.C. TERMINI E ABBREVIAZIONI

ACCOUNT: insieme di funzionalità, strumenti e contenuti attribuiti ad un utente in determinati contesti operativi, come siti web, determinati servizi su Internet ma anche per accedere alle più disparate applicazioni software.

ACTIVE DIRECTORY: Insieme di servizi di rete, adottati dai sistemi operativi Microsoft e gestiti da un domain controller. Esso si fonda sui concetti di dominio e di directory (che in inglese sta a significare "elenco telefonico"), ovvero la modalità con cui vengono assegnate agli utenti tutte le risorse della rete attraverso i concetti di: account utente, account computer, cartelle condivise, stampanti ecc... secondo l'assegnazione da parte dell'amministratore di sistema.

AGID (Agenzia per l'Italia digitale): è una agenzia pubblica italiana che svolge le funzioni ed i compiti ad essa attribuiti dalla legge al fine di perseguire il massimo livello di innovazione tecnologica nell'organizzazione e nello sviluppo della pubblica amministrazione e al servizio dei cittadini e delle imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia.

BACKUP: replicazione su un qualunque supporto di memorizzazione di materiale informativo archiviato nella memoria di massa dei computer, siano essi personal computer, workstation o server, al fine di prevenire la perdita definitiva dei dati in caso di eventi malevoli accidentali o intenzionali. Si tratta dunque di una misura di ridondanza fisica dei dati.

CLIENT: componente che accede ai servizi o alle risorse di un'altra componente detta server.

DHCP: protocollo di rete di livello applicativo che permette ai dispositivi o terminali di una certa rete locale di ricevere automaticamente ad ogni richiesta di accesso a una rete la configurazione necessaria per stabilire una connessione.

DNS: sistema utilizzato per la risoluzione di nomi dei nodi della rete in indirizzi IP.

Indirizzo IP: etichetta numerica che identifica univocamente un dispositivo detto *host* collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete.

LAN: una rete informatica di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.

NIS: Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi

RDBMS: Sistema per la gestione di database relazionali.

SERVER: componente o sottosistema informatico di elaborazione e gestione del traffico di informazioni che fornisce, a livello logico e fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate *clients*, cioè *clienti*) che ne fanno richiesta attraverso una rete di computer.

SINGLE SIGN ON: sistema di controllo d'accesso che consente ad un utente di effettuare un'unica autenticazione valida per più sistemi software o risorse informatiche alle quali è abilitato.

SISTEMA: qualsiasi apparecchiatura informatica, elettromedicale o dispositivo che si dovrà interfacciare/Integrare con l'infrastruttura IT di USL Umbria 1

VLAN: insieme di tecnologie che permettono di segmentare il dominio di broadcast, che si crea in una rete locale, in più reti locali logicamente non comunicanti tra loro, ma che condividono globalmente la stessa infrastruttura fisica di rete locale.

VPN: rete di telecomunicazioni privata aziendale sicura, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la rete Internet.

WSUS: Windows Server Update Services (WSUS) fornisce un servizio di aggiornamenti per i sistemi operativi Microsoft Windows e altri software Microsoft. E' un sistema di gestione locale che lavora combinato con Windows Update per dare agli amministratori dei sistemi la possibilità di gestire la distribuzione delle hotfix e degli aggiornamenti distribuiti, attraverso gli aggiornamenti automatici nei computer degli ambienti aziendali.

Art. 3.C. MODALITA' ESECUTIVE / CONTENUTI

I sistemi oggetto di fornitura dovranno essere coerenti con le politiche del presente documento nonché essere rispondenti alle normative in essere, o emanate in vigenza del presente contratto, in materia di sicurezza e privacy con particolare riguardo:

- alla Direttiva NIS (Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi);
- alle Misure Minime di Sicurezza ICT per la Pubblica Amministrazione diramate da AGID con circolare 18 aprile 2017;
- ai principi derivanti dal CAD-Codice dell'amministrazione digitale (con particolare riguardo all'art. 51 del D.lgs 82/05);
- al Regolamento europeo 2016/679 sulla protezione dei dati personali (GDPR) in virtù del quale il titolare del trattamento deve mettere in atto tutte le misure tecniche e organizzative adeguate per garantire che il trattamento dei dati personali.

Art. 3.1.C. ADEMPIMENTI DELL'AGGIUDICATARIO

L'aggiudicatario dovrà collaborare attivamente per quanto oggetto di fornitura alla produzione di documentazione che l'Azienda USL Umbria 1 è chiamata a redigere in ottemperanza alla vigente normativa in materia di sicurezza ICT e di privacy.

La fornitura dovrà essere sempre oggetto di apposito collaudo corredato dalla documentazione attestante la rispondenza del sistema alle presenti prescrizioni.

In particolare, per quanto riguarda dispositivi e sistemi medici/elettromedicali il collaudo sarà condizionato alla redazione e sottoscrizione da parte del fornitore di un accordo di responsabilità (responsibility agreement) redatto secondo i dettami della norma IEC 80001.

Tale documento dovrà fare riferimento allo scenario individuato nel contratto e alle specifiche configurazioni ed installazioni del sistema presso l'Azienda USL Umbria 1. Dovrà inoltre riportare i riferimenti alla "marcatura CE" dei dispositivi offerti ed al fatto che i requisiti essenziali di sicurezza non saranno inficiati dalla specifica installazione.

Art. 3.2.C. INTEGRAZIONE CON L'INFRASTRUTTURA IT DI USL UMBRIA 1

I sistemi oggetto di fornitura dovranno essere interfacciati o integrati con l'infrastruttura IT dell'Azienda USL Umbria 1 rispettando le direttive riportate di seguito e basate sullo specifico scenario di utilizzo.

I dispositivi dotati di connettività di rete (host) e che necessitano di collegamento alla rete dati per svolgere le proprie funzioni, potranno essere collegati solo se riconducibili ad uno dei seguenti scenari, mutuamente esclusivi:

- **Scenario 1:** Sistemi e/o dispositivi da integrare con la rete LAN o con i sistemi già presenti nell'Azienda USL Umbria 1 (es: integrazione con Active Directory o con altri software/sistemi già attivi) utilizzando in alcuni casi anche le risorse hardware preesistenti (es: hypervisor, infrastrutture cluster, ecc...).

- **Scenario 2:** Sistemi e/o dispositivi forniti dall'assegnatario che possono essere confinati ad una rete VLAN dedicata (isolamento totale dai sistemi dell'Azienda USL Umbria 1) e che prevedono l'utilizzo di hardware dedicato e non condiviso con quello preesistente.

L'aggiudicatario dovrà garantire la piena compatibilità dei sistemi forniti con l'infrastruttura descritta e in caso di incompatibilità completa dovrà proporre soluzioni analoga a quanto richiesto con il presente documento, in caso di incompatibilità parziale dovrà proporre un piano di adeguamento da attivare entro 3 mesi dal collaudo.

In entrambi i casi le soluzioni proposte dovranno essere presentate per iscritto ed essere validate dall'Azienda Sanitaria USL Umbria 1.

Art. 4.C. SCENARIO 1

In questo scenario i sistemi oggetto della fornitura sono strettamente integrati con l'infrastruttura IT dell'Azienda USL Umbria 1, sia dal punto di vista della rete che dei server, facendo affidamento in generale sulle infrastrutture di virtualizzazione e sui servizi di rete preesistenti.

Tale scenario è applicabile per esempio nel caso dell'implementazione di sistemi la cui fornitura non preveda l'installazione di hardware dedicato e può usufruire di sistemi di autenticazione basati su Active Directory.

Di seguito vengono riportate le caratteristiche peculiari dell'infrastruttura informatica dell'Azienda USL Umbria 1, definendo inoltre le specifiche di interfacciamento all'infrastruttura esistente alle quali i sistemi oggetto di fornitura dovranno adeguarsi.

SCENARIO 1 - Infrastruttura esistente

L'Azienda USL Umbria 1 dispone di un directory service aziendale basato su dominio Active Directory (AD).

Ogni account del directory service aziendale è associato ad almeno un gruppo di dominio (gruppi locali al dominio, domain local) corrispondente alla struttura amministrativa Azienda USL Umbria 1 di appartenenza.

Gli aggiornamenti di sistema per i client e per i server con sistema operativo Microsoft vengono distribuiti tramite il servizio WSUS.

Il protocollo di rete in uso nelle reti LAN dell'Azienda USL Umbria 1 è IPv4.

La risoluzione dei nomi è basata esclusivamente sul servizio DNS (Domain Name Service), integrato in AD, che accetta solo registrazioni sicure.

I backup dei sistemi, dei database, dei dati (presenti sui NAS e sui file server), delle macchine virtuali, dei registri di log dei sistemi saranno effettuati dai tecnici dell'Azienda USL Umbria 1 secondo specifici accordi con il fornitore ed in relazione alla specificità dei sistemi forniti.

Le postazioni di lavoro client dispongono di sistema operativo client Microsoft Windows di varie versioni.

L'applicativo antivirus aziendale è Sophos versione Central Intercept X Advanced.

Il controllo del traffico è realizzato tramite l'implementazione di apposite regole sui firewall aziendali redatte sulla base delle sole necessità di navigazione. Qualora la soluzione proposta necessiti di specifiche configurazioni, il fornitore dovrà collaborare con i tecnici dell'Azienda in fase di configurazione e fino al raggiungimento di adeguati livelli di sicurezza.

SCENARIO 1 – Virtualizzazione server

Gli eventuali server virtuali oggetto della fornitura dovranno essere compatibili con il sistema di virtualizzazione Nutanix versione 6.5.2 LTS.

Tutte le configurazioni relative ai sistemi e ai software in esse presenti dovranno rispecchiarne le politiche di gestione, comprese quelle di indirizzamento IP, di aggiornamento, di backup e di disaster recovery.

In relazione alle necessità potranno essere messe a disposizione dell'aggiudicatario una o più VM (macchine virtuali) rispecchiando l'architettura proposta, assegnando sufficienti risorse hardware in base alle specifiche necessità.

Dal punto di vista dei sistemi operativi, l'assegnatario potrà proporre al servizio informatico dell'Azienda USL Umbria 1 un ventaglio di possibili scelte al fine di selezionare la più opportuna sia in termini di compatibilità con la piattaforma di virtualizzazione in uso, che in termini di omogeneità con i sistemi operativi già presenti nell'infrastruttura.

In tutti i casi le licenze dei sistemi operativi (es: Windows Server) necessarie al funzionamento del sistema non sono da intendersi a carico del fornitore e non dovranno essere in alcun caso di tipo OEM, bensì licenze Retail/VLK intestate all'Azienda USL Umbria1.

In linea generale laddove si debbano implementare VM con sistema operativo Windows Server, sarà opportuno legare tali VM al dominio uslumbria1.it e conseguentemente al sistema di aggiornamento WSUS dell'Azienda USL Umbria 1.

Tali macchine verranno inserite in una apposita Organizational Unit (OU) relativa ai server oppure in una OU dedicata al fine di definire ed applicare su di esse le Group Policy di sicurezza ed autorizzazione concordate con l'Azienda USL Umbria 1.

Verrà applicata in ogni caso su tutte le OU la default domain policy.

Per quanto concerne la connettività di rete, ai server verrà assegnato un range di indirizzi IP statici nella rete della LAN aziendale o, se necessario, una subnet di rete dedicata.

SCENARIO 1 - Sistemi database RDBMS

Nel presente scenario, i dati acquisiti e generati dal sistema e/o i loro riferimenti, nonché tutti quelli direttamente o indirettamente necessari al funzionamento degli applicativi forniti, dovranno essere organizzati in uno o più RDBMS, che potranno essere istanziati sugli attuali server Microsoft SQL e Oracle di cui già dispone l'Azienda USL Umbria 1 o in nuovi RDBMS basati su altre piattaforme a discrezione dell'aggiudicatario, sempre previa valutazione con il servizio informatico al fine di stabilire l'eventuale conformità con le attuali politiche di sicurezza e compatibilità/sostenibilità con l'attuale sistema di backup e disaster recovery.

In quest'ultimo caso l'aggiudicatario dovrà farsi carico di fornire le licenze d'uso per gli RDBMS forniti e della gestione delle politiche di backup se non integrabili con l'attuale sistema di backup e disaster recovery.

SCENARIO 1 - Applicativi client/server o web-based

Nel presente scenario, gli applicativi destinati all'utilizzo da parte degli utenti dovranno essere basati su tecnologia client/server o web-based.

Gli eventuali applicativi destinati all'installazione lato client dovranno essere adeguati alle caratteristiche software e hardware delle postazioni di lavoro e dovranno garantire piena compatibilità con le policy del dominio Active Directory e con i software già installati nelle postazioni di lavoro.

.

Nel caso in cui non fosse possibile effettuare il deployment centralizzato di tali applicativi, l'installazione verrà effettuata – con analoghe caratteristiche qualitative e di risultato – da parte dell'aggiudicatario.

Per quanto concerne gli applicativi web, sarà necessario analizzarne e verificarne la compatibilità con i browser web e relativi plugin approvati dal servizio informatico per l'utilizzo dalle varie postazioni di lavoro dell'Azienda USL Umbria 1.

Gli applicativi web dovranno obbligatoriamente avere connessione protette tramite certificato fornito dall'Azienda (porta 443).

SCENARIO 1 – Sistemi client

Eventuali PC o apparati oggetto di fornitura, qualora dispongano di sistema operativo Microsoft Windows, dovranno essere configurati come membri del dominio uslumbria1.it in modo da essere conformi con le policy di dominio applicate ai computer dell'Azienda USL Umbria 1.

Nel presente scenario, se non diversamente comunicato dall'aggiudicatario, i sistemi operativi Microsoft Windows verranno aggiornati tramite WSUS installando tutte le patch rilasciate da Microsoft che verranno approvate dagli amministratori.

Le configurazioni di rete dei PC/apparati oggetto della fornitura dovranno garantire la compatibilità con il sistema di indirizzamento IP dinamico (DHCP) attivo in generale sui client dell'Azienda USL Umbria 1. Nel caso in cui l'architettura e le caratteristiche tecniche dei sistemi forniti impedissero tale configurazione, l'aggiudicatario sarà tenuto a redigere una relazione tecnica che giustifichi tale evenienza e sulla base della quale l'Azienda USL Umbria 1 si riserva di create sul servizio DHCP opportune e specifiche configurazioni (reservation).

Sulle postazioni dovrà essere installato l'antivirus Aziendale in considerazione del fatto che verranno applicate le politiche di aggiornamento/scansione standard dell'Azienda USL Umbria 1, a meno di eccezioni concordate con il servizio informatico.

Eventuali PC/apparati non Windows che non siano compatibili con l'Active Directory e che necessitano di connettività con la rete dati Azienda USL Umbria 1, verranno connessi alla stessa con specifici indirizzi IP statici assegnati dal servizio informatico dell'Azienda USL Umbria 1. La gestione del patching di tali sistemi è comunque obbligatoria ed è a carico dell'aggiudicatario.

SCENARIO 1 – VPN

In caso di necessità di interventi in teleassistenza da remoto da parte del personale tecnico dell'aggiudicatario durante il periodo di validità del contratto, l'accesso agli host oggetto di assistenza sarà garantito esclusivamente per mezzo dei sistemi VPN dell'Azienda USL Umbria 1.

Il personale tecnico potrà ottenere l'accesso al sistema VPN solo a fronte della compilazione del modulo specifico che dovrà essere inviato per validazione al servizio informatico dell'Azienda USL Umbria 1.

La connessione VPN dovrà essere di tipo client-to-site ed effettuata necessariamente utilizzando credenziali personali.

Nel caso in cui l'aggiudicatario non fosse in condizione di poter garantire tale configurazione per valide ragioni tecniche, sarà tenuto a redigere una relazione che giustifichi tale evenienza sulla base della quale l'Azienda USL Umbria 1 si riserverà di attivare connessioni di tipo site-to-site (es: tunnel IPSec). L'aggiudicatario dovrà garantire la tracciatura interna degli accessi effettuati da parte degli operatori che svolgono interventi in assistenza remota. L'Azienda USL Umbria 1 si riserva inoltre la facoltà di richiedere in qualsiasi momento il report di tali accessi.

Per rispondere ad eventuali esigenze di monitoraggio continuativo da remoto dello stato dei sistemi che sono oggetto della fornitura, lo strumento messo a disposizione dall'Azienda USL Umbria 1, a fronte di specifica configurazione, consentirà all'aggiudicatario di tenere costantemente sotto controllo lo stato dei servizi e dei dispositivi oggetto della fornitura.

SCENARIO 1 – Single Sign-On (SSO)

Tutti gli applicativi software forniti devono essere integrabili con l'LDAP messo a disposizione dal servizio Active Directory con livello di funzionalità minima 2012. Il collegamento dovrà passare tramite canale cifrato TLS/SSL debitamente autenticato tramite credenziali di sola lettura. L'integrazione del software oggetto della fornitura con il servizio LDAP di Active Directory andrà discussa di volta in volta con il servizio informatico al fine di fornire tutte le specifiche necessarie all'implementazione.

Altre soluzioni di SSO, autenticazione e account/identity management saranno consentite valutate dal Servizio informatico dell'Azienda USL Umbria 1.

Art. 5.C. SCENARIO 2

Questo scenario fa riferimento a tutti quei sistemi che, seppur installati all'interno dei locali dell'Azienda USL Umbria 1, non si interfacciano con la rete aziendale

SCENARIO 2 – CASISTICA A

I sistemi che non necessitano di connettività di rete (airgapped) dovranno essere comunque conformi alle disposizioni di legge in materia di sicurezza informatica e alla normative privacy vigenti.

La gestione del patching e della manutenzione di tali sistemi andrà esclusivamente gestita in locale, escludendo qualsivoglia sistema di gestione remota. Sarà pertanto onere del fornitore provvedere all'aggiornamento periodico dei sistemi tramite interventi on site in conformità alle misure minime indicate nell'Allegato n.1 – "Requisiti di conformità in ambito security"

SCENARIO 2 - CASISTICA B

I sistemi che non si devono integrare con la rete di USL Umbria 1 ma che necessitano di connettività di rete per svolgere le loro funzioni, verrà assegnata una specifica classe di indirizzi IP statici coerente con il piano di indirizzamenti dell'Azienda USL Umbria 1 e tali dispositivi verranno inseriti in una VLAN dedicata dalla quale potranno effettuare solo il traffico necessario per svolgere le funzioni richieste e il traffico relativo all'assistenza remota da parte del fornitore.

La disciplina del traffico verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali, stilate per rete IP e per porta, sulla base delle sole effettive necessità di traffico. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sui firewall.

Gli host forniti saranno soggetti a filtraggio della navigazione Internet. Potranno essere implementate specifiche eccezioni all'autenticazione basate su IP sorgente che consentiranno il traffico esclusivamente verso IP e porte specifiche. L'aggiudicatario dovrà fornire la massima collaborazione in tal senso all'Azienda USL Umbria 1 per la definizione delle suddette eccezioni.

Nel presente scenario l'aggiudicatario è responsabile in toto delle prescrizioni in ambito di sicurezza informatica e privacy, secondo quanto previsto dal quadro legislativo e normativo vigente, nonché dal presente documento; in particolare per quanto riguarda le politiche di: autenticazione, autorizzazione e accounting (AAA), di backup e disaster recovery, sugli aggiornamenti di sicurezza di tutti i software installati sugli host oggetto di assistenza, di protezione antivirus e da altre tipologie di cyber attacco.

Si specifica infine che, eventuali PC client o qualsivoglia dispositivo necessario al corretto e sicuro funzionamento dei sistemi oggetto di fornitura, dovranno essere gestiti interamente dal fornitore cui competerà il rispetto dei requisiti di legge in materia di sicurezza ICT.

I server o dispositivi di storage forniti dovranno essere conformi con gli standard per l'installazione a rack 19"; dovranno inoltre essere dotati di requisiti di ridondanza sufficienti a garantirne almeno la continuità operativa (es: doppio alimentatore, doppio storage controller, ecc...) e laddove possibile anche l'alta affidabilità (HA). Non dovranno infine essere utilizzati per alcun motivo come postazioni di lavoro da parte degli operatori.

Per quanto concerne l'accesso remoto tramite VPN ai dispositivi oggetto della fornitura, a fronte della connessione VPN effettuata tramite i sistemi messi a disposizione dall'Azienda USL Umbria 1, il collegamento ai singoli host oggetto di assistenza potrà avvenire con strumenti scelti dall'aggiudicatario, nel rispetto delle modalità previste dal quadro legislativo e normativo vigente, previa validazione degli strumenti stessi e della loro specifica configurazione da parte del servizio informatico dell'Azienda USL Umbria 1.

Qualora compatibile con i sistemi del fornitore, l'Azienda USL Umbria 1 può mettere a disposizione del fornitore uno strumento per consentire il monitoraggio continuativo da remoto dello stato di tali sistemi.

Art. 6.C. REQUISITI DI CONFORMITÀ IN AMBITO SECURITY

In entrambi gli scenari appena descritti sarà compito dell'aggiudicatario adeguare le specifiche dei sistemi oggetto della fornitura (e le relative modalità di gestione da parte degli amministratori) ai principi generali di sicurezza delle infrastrutture IT, garantendo la piena conformità alle prescrizioni indicate in questo documento, con particolare riferimento a quelle relative all'ambito della IT Security.

L'aggiudicatario dovrà garantire che sia l'architettura che gli elementi forniti vengano progettati, implementati e manutenuti nel tempo in modo da risultare conformi disposizioni previste dalla Direttiva NIS (Direttiva 2016/1148) e dalle misure minime di sicurezza ICT per la Pubblica Amministrazione, al fine di minimizzare il rischio informatico residuo sia di "attacchi ai sistemi" che di "attacchi dai sistemi".

Qui di seguito vengono esposte le indicazioni relative ai requisiti di conformità con le misure minime di sicurezza AGID applicabili al contesto delle forniture da parte di aziende esterne:

Inventario dei dispositivi: Nel caso in cui i dispositivi oggetto della fornitura vadano connessi alla rete (Scenario 1 o 2B) i dispositivi oggetto della fornitura andranno inventariati e tali dati di inventario andranno mantenuti aggiornati seguendo un processo formale di approvazione (vedi Allegato n.3). L'aggiudicatario dovrà compilare il modulo in allegato fornendo tutte le informazioni tecniche necessarie all'implementazione della fornitura in oggetto ed inviarlo al servizio informatico per l'approvazione e la valutazione di eventuali "non conformità". Sarà compito dell'aggiudicatario provvedere a comunicare tempestivamente eventuali modifiche o sostituzioni seguendo di volta in volta lo stesso iter di approvazione.

Laddove i dispositivi siano raggiungibili via rete, l'assegnatario sarà inoltre tenuto a comunicare al servizio informatico le modalità di scansione remota delle informazioni inerenti l'hardware e il software installati nel dispositivo (es: SNMP, WMI) e relative credenziali.

Elenco software autorizzati: il fornitore dovrà indicare preventivamente i sistemi operativi e i software che intenderà utilizzare nei propri dispositivi/sistemi sia come prima installazione che in caso di necessità di aggiornamenti a "major release" o in caso di sostituzione con altro software, seguendo anche in questo caso il processo formale di approvazione. I software non presenti nella lista di quelli autorizzati potranno essere installati solo a fronte di specifica richiesta e validazione da parte del servizio informatico.

Configurazioni sicure standard: le configurazioni dei dispositivi e dei software devono rispettare le configurazioni sicure standard, implementate nei clients tramite immagini di installazione preconfigurate e/o mediante group policies, le quali vengono applicate ai sistemi operativi Microsoft Windows sia server che client.

Nel caso di sistemi operativi non Microsoft o non agganciati al dominio, sarà cura del fornitore effettuare l'hardening ad-hoc dei propri sistemi tramite procedure che dovranno essere formalmente validate dal servizio informatico.

Connessioni protette per l'amministrazione remota: l'aggiudicatario dovrà configurare opportunamente i dispositivi o i software oggetto della fornitura affinché le operazioni di amministrazione da remoto possano avvenire per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri), utilizzando protocolli cifrati (es: https/SSH/RDP) che dovranno essere formalmente validati dal servizio informatico.

Verifica vulnerabilità: L'aggiudicatario deve verificare la presenza di eventuali vulnerabilità sia prima dell'installazione che dopo l'eventuale modifica/aggiornamento dei dispositivi e dei software oggetto

della fornitura. I sistemi collegati alla rete dell'Azienda USL Umbria 1 sono sottoposti periodicamente a verifica di vulnerabilità tramite appositi strumenti, pertanto, l'Azienda USL Umbria 1 verificherà che le vulnerabilità emerse dalle scansioni vengano risolte per mezzo di patch, o implementando opportune contromisure.

Patching dei dispositivi e degli OS: La politica di gestione degli aggiornamenti/patching dei dispositivi e dei sistemi operativi è naturalmente legata alla piattaforma in uso dallo specifico dispositivo fornito. In linea generale, nel caso in cui si tratti di sistemi basati su piattaforma Microsoft Windows sarà opportuno fare in modo che essi possano ricevere gli aggiornamenti dal server WSUS centralizzato già presente nell'Azienda USL Umbria 1, concordando con il servizio informatico dell'Azienda USL Umbria 1 dei time-slot periodici per consentire l'applicazione degli aggiornamenti sui propri sistemi e verificarne l'esito. In tutti gli altri casi, ovvero per le applicazioni proprietarie, per i sistemi Windows non legati al dominio, per i sistemi operativi non Windows o per tutti gli altri dispositivi, l'aggiudicatario si dovrà far carico della verifica della disponibilità ed installazione manuale delle patch, concordando con il servizio informatico dell'Azienda USL Umbria 1 dei time-slot periodici per consentirne l'esecuzione e la successiva verifica di funzionamento.

In linea generale le patch andranno installate entro 90gg dal rilascio, salvo la necessità di installarle con la massima urgenza nei casi in cui le patch vadano ad indirizzare e correggere bug o vulnerabilità ad alto livello di criticità.

Patching dei sistemi separati dalla rete (es: airgapped): In caso della fornitura di sistemi separati dalla rete, in particolare di quelli "airgapped", l'aggiudicatario dovrà farsi carico di assicurare l'aggiornamento tempestivo degli stessi. Anche in questo caso, in linea generale le patch andranno installate entro 90gg dal rilascio, salvo la necessità di installarle con la massima urgenza nei casi in cui le patch vadano ad indirizzare e correggere bug o vulnerabilità ad alto livello di criticità.

Strumentazione hardware: non è autorizzato l'uso di strumentazione in cui siano presenti sistemi in end of life. Nel caso in cui, nel corso del contratto, si verifichi una tale condizione il fornitore dovrà attivare tutte le misure necessarie affinché tale criticità venga risolta: sia che questo comporti la configurazione di una nuova macchina sia che richieda l'adeguamento dell'applicativo in uso;

Manutenzione del software: le applicazioni fornite devono rispondere ai requisiti previsti dalla normativa vigente e utilizzare sempre le ultime realise.

Gestione account privilegiati: L'Azienda USL Umbria 1 utilizza un software per la gestione e il tracciamento delle autorizzazioni a livello applicativo, compreso l'inventario degli amministratori di sistema.

I privilegi amministrativi vengono concessi solo ad utenti dotati delle competenze necessarie e di un incarico/contratto relativo alla configurazione dei sistemi, solo per consentire lo svolgimento di attività che richiedano specifici livelli di privilegi.

Le utenze personali devono essere formalmente autorizzate seguendo una specifica procedura di validazione da parte del servizio informatico.

Gli accessi amministrativi vengono tracciati nei registri di auditing e conservati su piattaforma di Log Management, sia per quanto concerne i sistemi federati con Active Directory che per i sistemi standalone. Al fine di consentire la corretta acquisizione dei log dai sistemi/dispositivi oggetto della fornitura l'aggiudicatario sarà tenuto a fornire al servizio informatico le relative specifiche tecniche.

Gestione account locali: Prima di collegare alla rete un nuovo dispositivo o prima di mettere in produzione un software, l'aggiudicatario dovrà provvedere a sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso. L'Azienda USL Umbria 1 si riserva la facoltà di effettuare periodicamente delle verifiche a campione al fine di verificare che le credenziali predefinite non siano ancora in uso.

System hardening: Le password delle utenze amministrative devono rispondere a criteri di elevata robustezza: devono essere soggette a limiti minimi di lunghezza (es: 14 caratteri), rotazione (password history > 10) e durata (password aging <90gg). NB: tale prescrizione dovrà essere applicata a tutte le utenze con privilegi amministrativi, coinvolte nella fornitura, indipendentemente dal fatto che siano locali, legate all'Active Directory o definite in qualsiasi altra piattaforma software.

Gestione account privilegiati: L'aggiudicatario dovrà fare distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali distinte. Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso. L'aggiudicatario dovrà inoltre conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.

Endpoint Protection: l'aggiudicatario dovrà provvedere ad installare l'antivirus centralizzato messo a disposizione dall'Azienda USL Umbria 1 (Sophos Endpoint Security) in tutti i dispositivi oggetto della fornitura, al fine di garantire adeguati livelli di protezione antivirus, firewall, IPS, controllo dei dispositivi

USB, controllo web e controllo delle applicazioni. Le politiche di configurazione della suite antivirus sono gestite centralmente e rispondono ai requisiti delle misure minime AGID ai punti sopraindicati; pertanto, eventuali eccezioni antivirus potranno essere create solo a fronte della verifica da parte del servizio informatico della conformità alle stesse. Non sarà inoltre possibile attivare l'utilizzo di servizi di posta elettronica esterni a quelli dell'Azienda USL Umbria 1.

Data Protection: In base allo scenario di rischio al quale potrà essere ricondotta la fornitura, dovrà essere garantita l'esecuzione di un backup periodico contenente le informazioni strettamente necessarie per il completo ripristino del sistema. Le modalità di esecuzione e la relativa pianificazione andranno concordate con il servizio informatico dell'Azienda USL Umbria 1 sulla base dello scenario applicabile. La riservatezza delle informazioni contenute nelle copie di sicurezza dovrà essere assicurata mediante adeguata protezione fisica dei supporti. Sarà inoltre necessario assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

Crittografia dati rilevanti: L'aggiudicatario dovrà effettuare un'analisi dei dati manipolati dalla propria applicazione o dal sistema oggetto della fornitura al fine di individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e quelli ai quali va applicata la protezione crittografica, al fine di concordare con il servizio informatico di USL Umbria 1 le modalità più opportune per l'adempimento di tale direttiva

RIFERIMENTI

- Regolamento UE 2016/679 (GDPR) – Regolamento generale sulla protezione dei dati
- Decreto Legislativo 30 giugno 2003, n° 196: "Codice in materia di protezione dei dati personali" e ss.mm.ii
- CAD Decreto Legislativo 82/2005 e ss.mm.ii
- Circolare Agid 18 Aprile 2017 n° 2: "Misure minime di sicurezza ICT per la PA"
- Direttiva NIS (Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi)
- Ulteriori norme in materia che dovessero essere emanate in corso di esecuzione del contratto

Art. 7 – Scenario 3 - Affidamenti servizi Cloud

In caso di affidamenti di servizio in Cloud il fornitore dovrà essere presente e/o dovrà avvalersi di un fornitore presente all'interno del market Place ACN (ex AGID).

Il livello minimo di sicurezza, capacità elaborativa, risparmio energetico e affidabilità deve rispondere alle disposizioni normative vigenti in materia e a quelle che dovessero essere emanate in corso di esecuzione del contratto. Tra le normative di riferimento si citano: GDPR, Direttiva NIS (Dlgs 65/2018), framework nazionale per la Cybersecurity e la data protection, linee guida o disposizioni ACN e AgID.

E' a carico del fornitore la messa in atto delle misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche che possano derivare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati nei sistemi oggetto di fornitura

In particolare il fornitore si impegna a :

- Censire le piattaforme e le applicazioni software in uso
- Garantire l'aggiornamento dei sistemi, dei database e degli applicativi
- Disporre di sistemi antivirus aggiornati e idonee misure di sicurezza
- Garantire una capacità elaborativa conforme agli standard del settore
- Individuare ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per le eventuali terze parti rilevanti (fornitori, clienti, partner)
- Effettuare peridiche attività di Risk Assestement relative agli asset e agli individui coinvolti
- Verificare che l'accesso agli asset logici e fisici, alle risorse dell'infrastruttura tecnologica e ai dati in generale è limitato al personale, ai processi e ai dispositivi autorizzati;
- Garantire che le modalità di autenticazione all'applicativo e/o ai sistemi sono commisurate al rischio della transizione;
- Garantire canali di comunicazione sicuri e criptati durante la trasmissione dei dati;

- Garantire la separazione tra gli ambienti di test e di sviluppo;
- Garantire che i backup delle informazioni siano eseguiti, amministrati e verificati con cadenza periodica.
  Il fornitore deve impegnarsi ad effettuare come minimo un backup giornaliero di tipo incrementale e uno settimanale di tipo completo;
- Garantire la manutenzione a caldo dei sistemi conformemente agli standard di mercato;
- Disporre di piani di risposta (Incident response e business Continuity) e recupero (Incident recovery e Disaster Recovery) in caso di incidente /disastro
- Effettuare periodiche attività di vulnerability assestement
- Disporre di un sistema di registrazione dei logs dei sistemi
- Disporre di un sistema di monitoraggio degli eventi che attraverso la correlazione dei dati consenta di rilevare tempestivamente incidenti o anomalie che possono avere di impatto sull'infrastruttura, sui sistemi e sui dati oggetto di fornitura
- Comunicare tempestivamente all'Azienda Sanitaria USL Umbria 1 eventuali anomalie o rischi rilevati
- Comunicare repentinamente e comunque non oltre le 24 ore il verificarsi di un data breach
- Collaborare con l'Azienda Sanitaria USL Umbria 1 in caso di Data Breach
- Garantire l'interoperabilità e la portabilità dei dati
- Garantire metriche di uptime pari al 99,00 %
- Consentire, se richiesta da parte dell'Azienda USL Umbria 1, verifiche di conformità da parte di proprio personale o di soggetti terzi (preventivamente individuati)

Il fornitore dovrà disporre di adeguata documentazione attestante le misure intraprese.

Dovrà inoltre produrre periodiche informazioni attestanti le attività di aggiornamento e monitoraggio dei sistemi, dei database e del software.

Al termine del contratto il fornitore deve impegnarsi restituire i dati oggetto del trattamento e a provvedere successivamente alla cancellazione definitiva dai propri sistemi

RIFERIMENTI

- Regolamento UE 2016/679 (GDPR) – Regolamento generale sulla protezione dei dati
- Decreto Legislativo 30 giugno 2003, n° 196: "Codice in materia di protezione dei dati personali" e ss.mm.ii
- CAD Decreto Legislativo 82/2005 e ss.mm.ii

- Circolare Agid 18 Aprile 2017 n° 2: “Misure minime di sicurezza ICT per la PA”
- Direttiva NIS (Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi)
- Regolamento recante “livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione” adottato dall’AgID con Determinazione n. 628/2021 del 15 dicembre 2021
- “Aggiornamento degli ulteriori livelli minimi di sicurezza, capacità elaborativa, e affidabilità delle infrastrutture digitali per la pubblica amministrazione e delle ulteriori caratteristiche di qualità, sicurezza, performance e scalabilità dei servizi cloud per la pubblica amministrazione, nonché requisiti di qualificazione dei servizi cloud per la pubblica amministrazione”: aggiornamento del regolamento adottata con determinazione ACN n. 307/2023 Determina ACN 307/2023
- Ulteriori norme in materia che dovessero essere emanate in corso di esecuzione del contratto