Cremona
COMUNE DI CREMONA
Area Segretario Generale
ICT - Agenda digitale

CAPITOLATO SPECIALE D'APPALTO

SERVIZIO DI SECURITY AND NETWORK AS A SERVICE (SECNAAS)

CON LICENZE E NOLEGGIO OPERATIVO

Indice generale

PREMESSA

Le sedi comunali con gli attuali fabbisogni di Sicurezza sono collegate con topologia a Stella con Centro in una delle sedi principali

Le sedi principali del Comune sono 8 e sono collegate Point-to-Point in fibra ottica, le sedi periferiche sono 20 e sono collegate con connettività pubblica e attraverso una VPN al Centro stella.

L'infrastruttura Intranet comunale è composta da diverse tipologie di apparati passivi, attivi e wifi di proprietà del Comune. In diverse sedi è attiva una rete Wi-Fi interna, nelle sedi principali la copertura Wi-Fi è completa.

In particolare la situazione è la seguente:

Sede	Armadi	Punti Rete
1	7	363
2	5	423
3	3	188
4	1	34
5	2	119
6	2	134
7	4	316
8	1	197

Per un totale di 135 apparati di rete di cui:

- 57 Switch,
- 78 Access Point

Il Comune di Cremona, inoltre, ha circa 610 Postazioni di Lavoro e circa 800 utenti di dominio.

Art. 1 OGGETTO DELL'APPALTO

L'oggetto dell'appalto riguarda il servizio di Security and Network as a Service (di seguito SECNaaS) che contempla:

- per la Cybersecurity: la fornitura in locazione operativa, la manutenzione delle apparecchiature hardware associate nonché tutti i servizi organizzativi, professionali e accessori che nel complesso concorrono a costituire il cosiddetto Servizio Security as a Service
- per la gestione delle Reti (Network) come oggetto integrato del sistema di sicurezza: la manutenzione delle apparecchiature hardware associate nonché tutti i servizi organizzativi, professionali e accessori che nel complesso concorrono a costituire il cosiddetto Servizio Network as a Service.

La prestazione è riconducibile ad un unico servizio al fine di evitare una disomogenità/disfunzionalità complessiva.

I servizi di Network Operating Center (NOC) e Security Operations Center (SOC) operano in sinergia. Mentre il NOC gestisce la funzionalità fisica e logica della rete LAN, il SOC interpreta i dati per la gestione degli incidenti di sicurezza.

1.1 Specifiche del servizio oggetto dell'appalto

Le specifiche del servizio oggetto dell'appalto sono esplicitate nella Tabella seguente:

Servizio	Articolo	Servizi oggetto dell'appalto
SEC	5.1	**Servizi di Sicurezza**
SEC_UTM_HW	5.1.1	Sicurezza periferica unificata noleggio operativo e attivazione degli apparati di sicurezza
SEC_UTM_SW	5.1.2	Servizi software di total security a bordo degli apparati
SEC_EPDR	5.1.3	Sicurezza postazioni
SEC_EPP	5.1.4	Sicurezza smartphone e tablet
SEC_IDP	5.1.5	Sicurezza autenticazioni
SEC_NDR	5.1.6	Sicurezza rete lan
SEC_DNSP	5.1.7	Protezione a livello DNS notebook
SEC_MDR	5.1.8	Servizio gestito di rilevamento e risposta agli eventi di cybersecurity (MDR)
ASSE	5.2	**Servizi di gestione asset**
ASSE_ONB	5.2.1	Onboarding del sistema
ASSE_LAN	5.2.2	Gestione degli apparati di rete lan
ASSE_RMM	5.2.3	Gestione remota dei dispositivi
ASSE_VA	5.2.4	Servizio di gestione continua delle vulnerabilità
ASSE_PATCH	5.2.5	Gestione patching dei dispositivi
ASSE_SOS	5.2.6	Servizio di sostituzione in emergenza
MON	5.3	**Servizi di Monitoraggio**
MON_NOC	5.3.1	Network Operation Center
MON_SOC	5.3.2	Security Operation Center
SP	5.4	**Servizi Professionali**
SP_POLC	5.4.1	Servizio di gestione policy e configurazioni
SP_MANA	5.4.2	Servizi di manutenzione
SP_STRA	5.4.3	Servizi di supporto strategico alle decisioni su networking e cybersecurity
FORM	5.5	**Servizi di Formazione**

L'appalto è costituito da un unico lotto in quanto: le caratteristiche tecniche dei prodotti a noleggio e dei servizi correlati oggetto di gara sono integrate tra di loro e funzionalmente connesse dal punto di vista tecnico per omogeneità e funzionalità.

Art. 2 Durata del contratto ed esecuzione anticipata

La durata del contratto di servizio (escluse le eventuali opzioni) è di 24 mesi con decorrenza presunta presunta dal 1 ottobre 2026 e scadenza presunta il 30 settembre 2028.

In casi eccezionali, il contratto in corso di esecuzione può essere prorogato per il tempo strettamente necessario alla conclusione della procedura di individuazione del nuovo contraente se si verificano le condizioni indicate all'articolo 120, comma 11, del Codice

degli appalti. In tal caso il contraente è tenuto all'esecuzione delle prestazioni agli stessi patti, prezzi e condizioni previsti nel contratto.

Al fine di consentire la transizione tra l'attuale configurazione del sistema e quella predisposta dall'aggiudicatario, a seguito dell'aggiudicazione definitiva, verrà indetto incontro di kick-off con l'operatore economico dal Responsabile del procedimento del Comune di Cremona. In tale incontro l'aggiudicatario presenterà il piano di dispiegamento (installazione e configurazione apparati, test di funzionalità, ecc.) al fine di garantire la piena operatività del servizio prevista entro e non oltre il ventesimo giorno lavorativo dalla data di aggiudicazione definitiva del presente contratto. Il piano di dispiegamento non potrà prevedere attività in carico all'ente diverse da quelle di mera informazione dello stato dell'arte.

In caso di ritardo nell'avvio della piena operatività del servizio saranno applicate le penali di cui all' Art. 9 - Inadempienze e penalità - del presente capitolato.

Si specifica che il riconoscimento del corrispettivo economico del presente Capitolato avranno decorrenza dalla messa in esercizio e dalla piena operatività di tutti i servizi e del loro collaudo (dove applicabile).

La Stazione appaltante si riserva, in caso di necessità e/o urgenza, la facoltà di chiedere l'avvio delle prestazioni contrattuali anche in pendenza della stipula del contratto, ai sensi dell'art. 17, commi 8 e 9, del D.Lgs. n. 36/2023

I servizi oggetto del presente capitolato sono da ritenersi servizi essenziali, e pertanto non sono passibili di interruzione con le conseguenti responsabilità penali e civili in capo al contraente. Nel caso di interruzione del servizio per causa imputabile all'aggiudicatario sarà pertanto applicata una penale come previsto all' Art. 9 - Inadempienze e penalità - del presente documento.

Art. 3 Modifica del contratto in fase di esecuzione

Opzione proroga: ai sensi dell'art. 120, co. 10 del D.Lgs. n. 36/2023, la stazione appaltante si riserva di prorogare il contratto per una durata massima pari a 24 mesi. L'importo stimato di tale opzione è pari a € 600.000 al netto di IVA. L'esercizio di tale facoltà è comunicato all'appaltatore almeno 2 mesi prima della scadenza del contratto.

Variazione fino a concorrenza del quinto dell'importo del contratto: Ai sensi dell'art. 120, comma 9, del D.Lgs. n. 36/2023, qualora in corso di esecuzione si renda necessario un aumento o una diminuzione delle prestazioni fino alla concorrenza del quinto dell'importo del contratto, la stazione appaltante può imporre all'appaltatore l'esecuzione alle condizioni originariamente previste. In tal caso, l'appaltatore non può far valere il diritto alla risoluzione del contratto. L'importo stimato di tale opzione, calcolato sul valore del contratto compresa la proroga contrattuale, è pari ad € 240.000,00= al netto dell'IVA.

Art. 4 Lotto unico, importo a base d'appalto e valore globale dell'affidamento

Ai sensi dell'art. 58, comma 2, del D.Lgs. n. 36/2023, si precisa che l'appalto è strutturato come lotto unico, in quanto il servizio presenta natura unitaria. La suddivisione in più lotti comporterebbe infatti una disomogeneità o disfunzionalità complessiva, tale da escludere qualsiasi convenienza, sia tecnica sia economica, nella ripartizione in due o più lotti.

Il corrispettivo a base d'appalto per la realizzazione del servizio oggetto dell'appalto è pari ad € 600.000,00 al netto dell'I.V.A.

Ai fini dell'art. 35 c. 4 del Codice dei contratti, il valore massimo stimato dell'appalto, considerando il rinnovo la proroga e tecnica è pari ad Euro 1.440.000 al netto dell' I.V.A.

Art. 5 Descrizione dell'appalto

Il seguente articolo illustra obiettivi, caratteristiche operative, criteri di applicabilità e attivabilità ed eventuali vincoli relativi a ciascun servizio previsto nell'appalto.

5.1 SEC - Servizi di Sicurezza

I servizi di Sicurezza di seguito descritti rappresentano i servizi e le soluzioni sia di tipo tecnologico che organizzativo e progettuale, che l'aggiudicatario deve soddisfare/erogare al fine garantire protezione completa per tutte le componenti di una rete aziendale. Grazie ad una soluzione di sicurezza all-in-one l'aggiudicatario deve implementare un unico punto di controllo di protezione delle minacce.

Gli apparati di sicurezza devono essere gestiti e collegati con le attuali tecnologie in uso al Comune: Watchguard Management Server (gestione centralizzata), Watchguard Dimension Server (log centralizzato anonimizzato) e Watchguard Cloud (integrazione con le altre componenti di sicurezza) o a componenti tecnologiche equivalenti (stesse funzionalità).

L'aggiudicatario dovrà altresì garantire il monitoraggio del traffico istantaneo e dei log con possibilità di analisi del traffico anche in un momento successivo, con una retention adeguata non inferiore al mese

5.1.1 SEC_UTM_HW - Sicurezza periferica unificata noleggio operativo e attivazione degli apparati di sicurezza

L'aggiudicatario deve predisporre un servizio di noleggio operativo di

- N. 2 Watchguard M4600 (velocità/porte ecc) o superiori o apparati equivalenti con moduli 8 SFP 1 GBit e moduli 4 SFP+ 10Gbit da predisporre nella sede del Servizio ICT e Agenda Digitale in modalità HA per tutta la durata contrattuale
- N. 22 WatchGuard Firebox T20 o superiori, o apparati equivalenti, per tutta la durata contrattuale per le sedi elencate nel documento "Sedi periferiche" in atti alla documentazione di gara.

Devono essere previste le licenze per le soluzioni software e per la totalità degli apparati hardware da gestire compresi eventuali server o altri sistemi necessari e/o utili per il funzionamento complessivo.

L'aggiudicatario deve garantire la consegna, l'installazione degli apparati UTM (presso la sede Servizio ICT) e dei firewall Firebox o equivalenti (per le sedi elencate nel documento “Sedi periferiche”) e la messa in esercizio complessiva con tutte le funzionalità di sicurezza (total security), garantendo la continuità delle policy e delle VPN attualmente attive presso il Comune.

In sede di Offerta Tecnica, verrà verificata l’aderenza ai seguenti requisiti minimi; il non raggiungimento dei requisiti minimi comporta l’esclusione del concorrent

Tipo	Requisito	Valore
Firewall sede centrale (centro stella)	Numero utenti	Almeno 1500
Firewall sede centrale (centro stella)	Numero interfacce	almeno 8 (1Gb) almeno 4 (10Gb Sfp+)
Firewall sede centrale (centro stella)	Throughput imix (firewall)	almeno 40 Gbps
Firewall sedi periferiche	Throughput imix (firewall)	almeno 510 Mbps
Firewall sedi periferiche	Numero interfacce	almeno 5 (1Gb)

Qualora i dispositivi hardware e i servizi software vengano messi in Eol (End of life) devono essere sostituiti in tempo utile con prodotti analoghi che dovranno essere messi a disposizione come rinnovo senza ulteriori costi a carico del Comune.

5.1.2 SEC_UTM_SW - Servizi software di total security a bordo degli apparati

L'aggiudicatario deve garantire l'erogazione dagli apparati di cui al punto 5.1.1, del servizio di Total Security o similari (in tal caso andrà fornita adeguata documentazione per verificarne la corrispondenza completa), che prevede l'attivazione dei sistemi qui sotto elencati e di ulteriori futuri sistemi di sicurezza relativi agli apparati in oggetto - che il costruttore svilupperà e metterà a disposizione per il mercato - senza ulteriori costi aggiuntivi per il Comune di Cremona. Attualmente i servizi sono:

- INTRUSION PREVENTION SERVICE (IPS) IPS utilizza schemi di attacco predefiniti denominati firme, continuamente aggiornati per analizzare il traffico presente su tutti i principali protocolli, così da fornire una protezione in tempo reale dalle minacce di rete, compreso lo spyware, le iniezioni SQL, gli script cross-site e l’overflow del buffer.
- SERVIZIO REPUTATION ENABLED DEFENSE (RED) Un servizio di verifica della reputazione basato su cloud che protegge gli utenti del web dai siti dannosi e dai botnet, migliorando al contempo in modo decisivo le risorse per l’elaborazione web.

- NETWORK DISCOVERY Un servizio per gli appliance/firewall di tipo Firebox che genera una mappa visiva di tutti i nodi della rete, consentendo all'amministratore di vedere con facilità quali sono i punti a rischio.
- GATEWAY ANTIVIRUS (GAV) Un servizio che sfrutta schemi di attacco predefiniti (firme) costantemente aggiornati per identificare e bloccare le fonti note di spyware, virus, cavalli di Troia, worm, rogueware e minacce combinate, comprese le nuove varianti dei virus già noti. Completa il servizio, un'analisi euristica che consenta di individuare le strutture e le operazioni sospette sui dati per fare in modo che i virus sconosciuti non possano aggirare i controlli.
- FILTRO URL DI WEBBLOCKER Un servizio volto a bloccare in modo automatico i siti dannosi, gli strumenti di filtro dettagliati del contenuto e degli URL di WebBlocker che permettono di bloccare i contenuti inappropriati, conservare l'ampiezza di banda di rete e migliorare la produttività dei dipendenti.
- APPLICATION CONTROL un servizio che consente di bloccare o ridurre selettivamente l'accesso alle applicazioni in base al reparto, alla mansione e all'orario di lavoro dell'utente e quindi vedere in tempo reale a quali risorse di rete stanno accedendo gli utenti.
- SPAMBLOCKER Rilevamento in tempo reale dello spam per la protezione dalle infezioni. Il nostro spamBlocker è così veloce ed efficace da poter analizzare fino a 4 miliardi di messaggi al giorno.
- APT BLOCKER: PROTEZIONE AVANZATA DAL MALWARE APT Blocker utilizza una sandbox pluripremiata di ultima generazione per rilevare e bloccare gli attacchi più sofisticati, compresi il ransomware, le minacce zero-day e altri malware avanzati.
- DATA LOSS PREVENTION (DLP) Questo servizio previene la perdita di dati accidentale o intenzionale eseguendo la scansione di file di testo e di tipi di file comuni alla ricerca di informazioni sensibili che stanno per uscire dalla rete.
- DIMENSION COMMAND Un servizio che traduce i dati acquisiti da tutte gli appliance della rete in informazioni facilmente usufruibili riguardanti la rete e le minacce. Il servizio deve offrire quanto necessario per implementare azioni mirate a neutralizzare le minacce all'istante da un'unica console centralizzata.
- THREAT DETECTION AND RESPONSE Un servizio di correlazione degli eventi di sicurezza della rete e degli endpoint con informazioni sulle minacce per individuare, classificare e consentire un'azione immediata con cui fermare gli attacchi malware. Miglioramento della visibilità attraverso l'evoluzione dell'attuale modello di sicurezza oltre la prevenzione, fino a includere funzionalità di correlazione, rilevamento e risposta.
- Filtering DNS: Un servizio per rilevare le richieste DNS dannose e bloccare l'accesso ai siti, reindirizzando l'utente su una pagina sicura in cui vengono fornite informazioni e avvertenze sui rischi e i segnali degli attacchi di phishing. trasformando questi eventi in momenti di formazione per i dipendenti che sono molto efficaci nel comunicare i rischi dei clic sui link di phishing.

- INTELLIGENT AV: Un servizio che faccia uso di una soluzione anti-malware senza firma che si basa sull'intelligenza artificiale per automatizzare l'individuazione di malware sfruttando analisi statistiche approfondite,in grado di classificare il malware corrente e zero day in pochi secondi.
- ACCESS PORTAL: Un servizio che offrà una soluzione VPN senza client che fornisce accesso remoto sicuro alle applicazioni Web comuni che utilizzano le tecnologie HTML, HTML5 e JavaScript. Non deve essere necessario installare un client software o hardware, ma gli utenti devono attraverso il solo browser Web connettersi alle seguenti risorse tramite il portale di accesso: applicazioni web esterne di terze parti, sessioni RDP e SSH alle risorse locali, applicazioni interne (reverse proxy), Microsoft Exchange services (reverse proxy). Deve essere possibile eseguire il proxy delle connessioni HTTPS alle applicazioni del portale di accesso. Deve essere possibile specificare a quali applicazioni e gruppi di applicazioni possono connettersi utenti e gruppi di utenti. Inoltre deve essere possibile configurare il Single Sign-On (SSO) con il protocollo di autenticazione SAML ed un proprio identity provider.

Qualora i dispositivi hardware e i servizi software vengano messi in Eol (End of life) devono essere sostituiti in tempo utile con prodotti analoghi che dovranno essere messi a disposizione come rinnovo senza ulteriori costi a carico del Comune.

5.1.3 SEC_EPDR - Sicurezza postazioni

Il Comune di Cremona dispone all'incirca delle seguenti postazioni di lavoro:

- 230 notebook
- 380 desktop

L'aggiudicatario deve fornire protezione end point protection, threat detection and response, in modalità cloud per ogni postazione di lavoro notebook e desktop, quindi per circa 610 postazioni.

La piattaforma deve fornire il massimo della protezione con una complessità minima, offrire in unica soluzione le più avanzate tecnologie di protezione per endpoint e integrare le tecnologie per il rilevamento e la risoluzione delle minacce.

I prodotti e i servizi per la sicurezza devono essere incentrati sull'utilizzatore finale per proteggere i dispositivi e le reti con cui si effettua la connessione da spam, phishing, malware, siti web malevoli e altre minacce compresi gli attacchi "zero day" non ancora noti.

Il servizio di rilevamento e risposta alle minacce si deve basare su quattro principi:

1. monitoraggio continuo mediante l'analisi di tutti gli eseguibili che permette l'esecuzione delle sole azioni affidabili proteggendo dai file inaffidabili.
2. rilevamento di attacchi mirati per ridurre la superficie con possibilità di essere infettata.
3. rilevamento intelligente e automatizzato delle minacce informatiche avanzate.

4. risposta rapida ai file e agli applicativi malevoli per evitare danni e ridurre costi di intervento.

La soluzione deve offrire anche sistemi di rilevamento delle intrusioni (IDS), firewall, controllo dei dispositivi, protezione della posta elettronica, filtro dei contenuti e URL.

La piattaforma antivirus deve essere un'efficace soluzione di sicurezza nativa per il cloud che centralizza gli antivirus di nuova generazione di tutti i desktop e notebook. Questa protezione completa deve coprire tutti i vettori: rete (firewall), e-mail, Web e dispositivi esterni. L'agente installato sui dispositivi deve essere leggero affinché possa esercitare un impatto minimo sulle prestazioni degli endpoint, gestiti da un'unica architettura cloud ed offrire protezione da applicazioni dannose, malware, phishing, ransomware e trojan e anche da script e macro dannose contenute nei documenti di Office.

Dato che il numero delle postazioni di lavoro può subire fluttuazioni nel tempo e nella composizione è necessario che l'aggiudicatario consenta al Comune di avere un certo grado di flessibilità circa il numero di licenze di volta in volta attive.

Durante il periodo contrattuale le postazioni potranno fluttuare nei seguenti range:

Notebook	valore soglia minimo	valore soglia massimo	periodo attivazione	
			da	a
	200	350	attivazione contratto	scadenza cotratto

Desktop	valore soglia minimo	valore soglia massimo	periodo attivazione	
			da	a
	301	400	attivazione contratto	scadenza cotratto

Le attivazioni potranno essere richieste fino a 24 ore prima e dovranno essere fatturate solo le licenze attivate al Comune. Il comune avrà facoltà di richiedere l'assegnazione delle licenze di cui abbisogna, variandone la quantità dalla soglia minima alla soglia massima, sia in termini incrementali che decrementali, con cadenza trimestrale.

5.1.4 SEC_EPP - Sicurezza smartphone e tablet

Il Comune di Cremona dispone all'incirca dei seguenti dispositivi mobili:

- 270 smartphone
- 40 tablet

L'aggiudicatario deve fornire, protezione end point protection, in modalità cloud per ogni dispositivo mobile, quindi per circa 310 postazioni.

La piattaforma deve fornire il massimo della protezione con una complessità minima, offrire in unica soluzione le più avanzate tecnologie di protezione per endpoint e integrare le tecnologie per il rilevamento e il blocco delle minacce.

I prodotti e i servizi per la sicurezza devono essere incentrati sull'utilizzatore finale per proteggere i dispositivi e le reti con cui si effettua la connessione da spam, phishing, malware, siti web malevoli e altre minacce.

Il servizio di rilevamento delle minacce si deve basare su quattro principi:

1. monitoraggio continuo mediante l'analisi di tutti gli eseguibili che permette l'esecuzione delle sole azioni affidabili proteggendo dai file inaffidabili.
2. rilevamento di attacchi mirati per ridurre la superficie con possibilità di essere infettata.
3. blocco dei file e degli applicativi malevoli per evitare danni e ridurre costi di intervento.

La piattaforma antivirus deve essere un'efficace soluzione di sicurezza nativa per il cloud che centralizza gli antivirus di nuova generazione di tutti gli smartphone e i tablet. L'agente installato sui dispositivi deve essere leggero affinché possa esercitare un impatto minimo sulle prestazioni degli endpoint, gestiti da un'unica architettura cloud ed offrire protezione da applicazioni dannose, malware, phishing, ransomware e trojan e anche da script e macro dannose.

Dato che il numero degli endpoint di lavoro può subire fluttuazioni nel tempo e nella composizione è necessario che l'aggiudicatario consenta al Comune di avere un certo grado di flessibilità circa il numero di licenze di volta in volta attive.

Durante il periodo contrattuale le postazioni potranno fluttuare nei seguenti range:

Smartphone	valore soglia minimo	valore soglia massimo	periodo attivazione	
			da	a
	60	400	attivazione contratto	scadenza contratto

Tablet	valore soglia minimo	valore soglia massimo	periodo attivazione	
			da	a
	10	100	attivazione contratto	scadenza contratto

Le attivazioni potranno essere richieste fino a 24 ore prima e dovranno essere fatturate solo le licenze attivate al Comune. Il comune avrà facoltà di richiedere l'assegnazione delle licenze di cui abbisogna, variandone la quantità dalla soglia minima alla soglia massima, sia in termini incrementali che decrementali, con cadenza trimestrale.

5.1.5 SEC_IDP - Sicurezza autenticazioni

Il Comune di Cremona ha attivato la soluzione AuthPoint di Watchguard per affrontare una delle principali lacune della sicurezza con l'autenticazione a più fattori (MFA) su una piattaforma cloud compatibile con molti sistemi di autenticazione.

L'aggiudicatario deve quindi garantire il servizio SEC_IDP con le seguenti quantità e tempistiche:

Servizio SEC_IDP	valore soglia utenze minimo	valore soglia utenze massimo	periodo attivazione	
			da	a
	501	900	attivazione contratto	scadenza contratto

Le attivazioni potranno essere richieste fino a 24 ore prima e dovranno essere fatturate solo le licenze attivate/assegnate al Comune. Il comune avrà facoltà di richiedere l'assegnazione delle licenze di cui abbisogna, variandone la quantità dalla soglia minima alla soglia massima, sia in termini incrementali che decrementali, con cadenza trimestrale.

Il servizio è richiesto per l'intera durata contrattuale e deve contemplare anche supporto tecnico e il monitoraggio degli accessi. L'accesso alla console di gestione dovrà essere consentito anche ai tecnici ICT del Comune.

5.1.6 SEC_NDR - Sicurezza rete lan (sedi principali e numero apparati)

L'aggiudicatario dovrà fornire un servizio Watchguard NDR (Network Detection & Response) o equivalente. Tale servizio monitora in tempo reale il traffico di rete interno, esterno e ambienti cloud, per individuare e rispondere automaticamente ad attività sospette o minacce avanzate attraverso analisi avanzate dei dati grezzi, del traffico di rete e dei metadati, costruendo modelli di comportamento "normale" per rilevare deviazioni o minacce nascoste, movimenti laterali, attacchi zero-day ed esfiltrazione di dati e offre capacità di risposta agli incidenti, come il blocco automatico del traffico sospetto.

Tutte le sedi principali ed eventualmente gli ambienti cloud dovranno essere oggetto dell'analisi del traffico di rete, in particolare si specifica che dovrà essere analizzato anche tutto quel traffico intra sede che rimane sugli apparati periferici senza raggiungere i core switch del centro stella.

Le funzionalità devono comprendere

- Modellazione del traffico di rete in modo che le anomalie si distinguano e il rilevamento si verifichi su base comportamentale piuttosto che cercando firme specifiche; ciò richiede Machine Learning, analisi avanzate e modelli di intelligenza artificiale per individuare minacce avanzate;
- Tasso di falsi positivi costantemente basso una volta che la soluzione è stata correttamente messa a punto, garantendo al SOC risultati affidabili;

- Capacità di aggregare e correlare gli eventi con la telemetria endpoint e identità, in modo da fornire una visione unificata del rischio e generando allert di "incidenti strutturati", facilitando la prioritizzazione dei rischi e l'indagine sulle minacce;
- capacità di investigazione e risposta centralizzate su un'unica console, meglio se integrata con le altre componenti di sicurezza;
- completa compatibilità con ambienti ibridi e multi-cloud;
- Capacità di contenere o bloccare le minacce con risposte automatizzate, semplificando le operazioni di sicurezza
- strumenti per la produzione di reportistica di sicurezza e, ove richiesto, elementi a supporto della conformità normativa.

L'aggiudicatario deve quindi garantire il servizio SEC_NDR con le seguenti quantità e tempistiche:

Servizio SEC_NDR	soglia minima garantita asset/ip monitorati	soglia massima asset/ip monitorati	periodo attivazione	
			da	a
	1001	1500	attivazione contratto	scadenza cotratto

Le attivazioni potranno essere richieste fino a 24 ore prima e dovranno essere fatturate solo le licenze attivate/assegnate al Comune. Il comune avrà facoltà di richiedere l'assegnazione delle licenze di cui abbisogna, variandone la quantità dalla soglia minima alla soglia massima, sia in termini incrementali che decrementali, con cadenza trimestrale.

Il servizio è richiesto per l'intera durata contrattuale e deve contemplare anche supporto tecnico e il monitoraggio degli accessi. L'accesso alla console di gestione dovrà essere consentito anche ai tecnici ICT del Comune.

La soluzione deve assicurare semplicità di implementazione, ridotto impatto sull'infrastruttura dell'Ente e capacità di integrazione con gli altri servizi di rilevamento e risposta.

Il servizio dovrà essere necessariamente attivo su tutti i device che verranno concordati con l'ente (a titolo esemplificativo ma non esaustivo: pc, notebook, switch, router, firewall,...). Non è richiesto per i dispositivi quali smartphone e tablet.

5.1.7 SEC_DNSP - Protezione a livello DNS notebook

L'aggiudicatario deve estendere il servizio di sicurezza WatchGuard "protezione a livello DNS" o equivalente ai dispositivi esterni alla rete attraverso un servizio di protezione a livello DNS implementato sulla postazione di lavoro per gli utenti in mobilità. Il servizio deve monitorare le richieste DNS in uscita e interrompere le comunicazioni dei dispositivi con l'infrastruttura dannosa, quando viene effettuato un tentativo di connessione a un sito

pericoloso, bloccando la connessione e facendo indagini della minaccia. Devono essere bloccate automaticamente le eventuali violazioni, gli attacchi di phishing e i tentativi di estrazione dei dati.

Il servizio deve includere l'attivazione di una formazione mirata all'utente che cade nel phishing, relativa ai segnali d'attacco.

L'aggiudicatario deve garantire il servizio SEC_DNSP con le seguenti quantità e tempistiche:

Servizio SEC_DNSP	valore soglia minimo	valore soglia massimo	periodo attivazione	
			da	a
	201	350	attivazione contratto	scadenza cotratto

Le attivazioni potranno essere richieste fino a 24 ore prima e dovranno essere fatturate solo le licenze attivate/assegnate al Comune. Il comune avrà facoltà di richiedere l'assegnazione delle licenze di cui abbisogna, variandone la quantità dalla soglia minima alla soglia massima, sia in termini incrementali che decrementali, con cadenza trimestrale.

5.1.8 SEC_MDR - Servizio gestito di rilevamento e risposta agli eventi di cybersecurity (MDR)

L'aggiudicatario dovrà fornire un servizio Watchguard MDR (Managed Detection and Response) o equivalente completamente gestito, in grado di garantire protezione continua 24/7 su dispositivi, identità utente, applicazioni e infrastrutture cloud e traffico di rete interno (intra vlan su tutte le sedi) ed esterno (navigazione in ingresso ed in uscita). Il servizio deve includere monitoraggio costante, analisi esperta e risposta automatizzata e manuale alle minacce, con riduzione dei falsi allarmi e intervento rapido per contenere attacchi reali.

La soluzione proposta dovrà fornire visibilità centralizzata tramite un portale unico, con timeline degli incidenti, report di protezione, supporto per compliance normativa e assicurazioni cyber.

Il fornitore deve garantire onboarding rapido, scalabilità semplice su ambienti ibridi o multi-tool, e la disponibilità di un Technical Account Manager dedicato, che fornisca interpretazione delle attività SOC, revisioni regolari e supporto nella rendicontazione della sicurezza.

La soluzione dovrà essere basata sulla piattaforma WatchGuard MDR o equivalente, assicurando la copertura completa di endpoint, identità utente, navigazione rete interna ed esterna e servizi cloud, con capacità di risposta proattiva e contenimento rapido delle minacce.

Il servizio deve comprendere:

- verifica e classificazione degli alert mediante analisti specializzati;

- attivazione di azioni di risposta quali isolamento dell'endpoint compromesso, blocco delle comunicazioni sospette, disattivazione di account o altre misure di contenimento;
- comunicazione tempestiva all'Ente e fornitura delle informazioni necessarie al ripristino;
- report periodici sullo stato di sicurezza, analisi post-evento e raccomandazioni per il miglioramento della postura di sicurezza;
- gestione multi-tenant e piattaforma unificata per la consultazione degli eventi e delle attività di risposta.

Tutte le attività di contenimento, analisi e supporto alla risoluzione devono essere incluse nel servizio senza prevedere livelli aggiuntivi di licenza o costi accessori per funzionalità fondamentali.

Il servizio è richiesto per l'intera durata contrattuale e deve contemplare anche supporto tecnico e il monitoraggio degli accessi. L'accesso alla console di gestione dovrà essere consentito anche ai tecnici ICT del Comune.

Il servizio dovrà essere necessariamente attivo su tutti i device che verranno concordati con l'ente (a titolo esemplificativo ma non esaustivo: pc, notebook, switch, router, firewall,...). Non è richiesto per i dispositivi quali smartphone e tablet.

5.2 ASSE - Servizi di Gestione Asset

L'aggiudicatario deve fornire un Servizio di Gestione Asset che comprenda:

- La gestione dei dispositivi di rete (Router, Switch, AP, ...)
- La gestione remota e proattiva dei dispositivi (PC, Notebook, ...)
- L'analisi delle vulnerabilità e il relativo patching remoto e ove possibile automatizzato

5.2.1 ASSE_ONB - Onboarding del sistema rete locale

L'aggiudicatario dovrà fornire il servizio di on-boarding che prevede: la pulizia di ogni armadio di rete e dispositivo attivo presso le sedi dell'ente, il censimento degli armadi ed inventario in sistemi digitali integrato con i sistemi di gestione dell'ente, il censimento dei dispositivi e tagging, il setup e gestione dei sistemi di monitoraggio (SNMP)

Le azioni di on-boarding e la situazione per ogni locale tecnico dovrà essere verificata e validata dal servizio ICT. All'inizio dell'affidamento verrà steso un piano di revisione di tutti i locali tecnici. L'aggiudicatario dovrà stendere una relazione sulle problematiche e sugli interventi da realizzare per una corretta gestione di ogni locale tecnico in ordine a: sicurezza fisica (accesso, pulizia, raffrescamento), cablaggio ordinato e stato degli apparati. Essendo gli armadi di rete un asset strategico, l'aggiudicatario in collaborazione con il Servizio ICT provvederà a stendere una scheda informativa in forma di check-list per ogni locale e armadio di rete e successivamente a inventariare la situazione rilevando lo stato di efficienza dei dispositivi e le criticità da monitorare attraverso disciplinari tecnici. L'aggiudicatario è tenuto a rendicontare anche lo stato di efficienza dei dispositivi di rete.

5.2.2 ASSE_LAN - Gestione degli apparati di rete lan

Il servizio consiste in monitoraggio, manutenzione, assistenza e configurazione di tutti gli apparati di rete LAN di proprietà dell'ente (router, switch e access point) presenti nelle sedi principali e nelle sedi periferiche. Non sono previsti limiti al numero degli interventi a cui l'aggiudicatario è chiamato.

Il servizio deve permettere il controllo della funzionalità fisica e logica e delle performance della rete.

l'aggiudicatario deve dare comunicazioni tempestive al Direttore dell'Esecuzione del Contratto o altro referente del Comune tramite e-mail e, in caso di priorità molto alta, anche tramite telefono, di eventuali segnalazioni inerenti ogni anomalia verificatasi durante l'esercizio. In caso di problemi bloccanti, l'aggiudicatario deve intervenire, previo accordo, per eliminare il guasto e nel rispetto degli SLA rappresentati all'art. 6, ove non diversamente specificato, o di loro miglioramenti in caso di offerta migliorativa dell'aggiudicatario.

Le attività previste per erogare il seguente servizio si dividono in 4 macro-categorie:

- **Attività di manutenzione programmata per il mantenimento dell'adeguato livello di funzionalità e sicurezza:**

  In questa casistica rientrano le attività di aggiornamento continuativo dei sistemi e le attività volte a garantire una pronta correzione dei malfunzionamenti. L'aggiudicatario verifica con continuità l'esistenza di patch, fix pack, release e aggiornamento firmware rilasciate dal produttore originario che devono essere installate sugli apparati del Comune, al fine di adeguarli agli ultimi aggiornamenti in tema di sicurezza e funzionalità. L'attività di aggiornamento deve essere concordata col Direttore dell'Esecuzione del Contratto o altro referente dell'Ente;

  Il servizio deve rispettare i seguenti parametri per garantire gli SLA:

  - tempo di presa in carico = entro 1 h rispetto al piano orario con eventuale slittamento al next business day in caso di richiesta fuori orario di lavoro
  - tempo di intervento garantito = massimo 24 h solari

- **Attività di manutenzione a seguito di guasto o malfunzionamento:**

  In questa casistica rientrano le attività correlate al ripristino delle funzionalità anche attraverso attività di supporto on-site che l'aggiudicatario deve garantire. Le attività sono governate dal Servizio ICT del Comune di Cremona che in qualità di proprietario degli apparati mantiene e rende disponibile all'aggiudicatario il magazzino, consentendo la massima tempestività nella gestione di possibili sostituzioni dell'hardware. L'aggiudicatario interviene in caso di necessità coordinando le attività con il Servizio ICT dell'ente.

  Nel caso in cui situazioni impreviste vadano ad esaurire la disponibilità di switch e access point a magazzino, l'aggiudicatario dovrà predisporre la fornitura degli apparati necessari alla manutenzione e al corretto funzionamento della rete utilizzando il servizio ASSE_SOS (5.2.6)

Il servizio deve rispettare i seguenti parametri per garantire gli SLA:

- tempo di presa in carico = entro 1 h rispetto al piano orario con eventuale slittamento al next business day in caso di richiesta fuori orario di lavoro
- tempo di intervento garantito = massimo 24 h solari

- **Attività di monitoraggio e gestione del parco installato:**

  Per tutta la durata del contratto il corretto funzionamento degli apparati di rete LAN e le relative configurazioni dovranno essere costantemente monitorati mediante l'ausilio di una o più sonde network direttamente dall'unico punto di controllo, intregrato in questo progetto. In presenza di un'anomalia, un malfunzionamento o traffico anomalo rispetto alle policy definite, verranno automaticamente aperti ticket per le successive azioni correttive.

  Il servizio deve rispettare i seguenti parametri per garantire gli SLA:

  - tempo di presa in carico = entro 1 h entro rispetto al piano orario con eventuale slittamento al next business day in caso di richiesta fuori orario di lavoro
  - tempo di intervento garantito = massimo 24 h solari

- **Attività di adeguamento rispetto a cambiamenti architetturali fino a 4 ore:**

  Qualora l'ente intenda procedere ad adeguamenti infrastrutturali, cambiamenti architetturali, mobilità di risorse umane e/o tecnologiche, l'aggiudicatario è chiamato alla mobilità degli apparati e all'adeguamento delle configurazione al fine di ripristinare il corretto funzionamento in base alla nuova disposizione definita dall'ente, se le attività richieste sono espletabili in un tempo compreso in 4 ore. L'ente e l'aggiudicatario concordano le attività attraverso i responsabili/referenti del contratto.

  Nel caso di attivazione di nuova sede o spostamento straordinario di sedi con numerosi apparati da movimentare, tali da richiedere un tempo maggiore alle 4 ore, il fornitore attingerà al budget delle risorse a consumo fatturando i relativi costi.

  Il servizio deve rispettare i seguenti parametri per garantire gli SLA:

  - tempo minimo di pianificazione dell'ente: 5 giorni lavorativi – L'ente deve comunicare all'aggiudicatario i cambiamenti da attuare almeno 5 giorni prima dell'avvio di tali cambiamenti
  - l'aggiudicatario deve attenersi al giorno e all'ora concordata per eseguire l'intervento

Viene richiesto un aggiornamento della documentazione del patching rispetto alle porte degli switch e alla terminazione negli uffici ogni qual volta l'aggiudicatario è chiamato ad un intervento sulla rete.

5.2.3 ASSE_RMM - Gestione remota dei dispositivi

Al fine di supportare efficacemente il servizio di gestione remota delle PdL, degli apparati di rete e di tutti i dispositivi collegati, anche in relazione all'effettiva capacità di limitare al minimo gli interventi di gestione in locale o in telelavoro, l'aggiudicatario dovrà predisporre e rendere disponibili al personale del Servizio ICT del Comune ed agli operatori del Service desk, collaboratori del Comune, gli opportuni strumenti operativi adatti allo scopo. Lo strumento deve essere manutenuto alla versione più recente.

Lo strumento dovrà permettere queste attività:

- controllo dello stato di accensione: con l'apparecchiatura accesa e il sistema operativo caricato, da console remota deve essere possibile eseguire il comando di spegnimento e verificare che l'apparecchiatura esegua la chiusura del sistema operativo e l'arresto del sistema;
- controllo remoto: il software dovrà permettere di prendere il controllo pieno del desktop remoto, mantenendo aperta la sessione in modo che l'utente della PdL possa visualizzare costantemente le operazioni eseguite remotamente. Durante la sessione remota dovrà essere possibile lo scambio file bidirezionale e la chat testuale tra controllato e controllante. L'accesso remoto alla macchina dovrà essere possibile solo da parte di utenti autorizzati in possesso di credenziali di amministratore e su accettazione dell'utente finale;
- controllo remoto in sicurezza da parte dei fornitori di software del comune per attività di supporto agli utenti;

Il servizio ASSE_RMM dovrà coprire le postazioni portatili e fisse.

L'aggiudicatario deve quindi garantire il servizio ASSE_RMM con le seguenti quantità e tempistiche:

Servizio ASSE_RMM	valore soglia minimo	valore soglia massimo	periodo attivazione	
			da	a
	501	750	attivazione contratto	scadenza contratto

Le attivazioni potranno essere richieste fino a 24 ore prima e dovranno essere fatturate solo le licenze attivate/assegnate al Comune. Il comune avrà facoltà di richiedere l'assegnazione delle licenze di cui abbisogna, variandone la quantità dalla soglia minima alla soglia massima, sia in termini incrementali che decrementali, con cadenza trimestrale.

5.2.4 ASSE_VA - Servizio di gestione continua delle vulnerabilità

L'aggiudicatario dovrà fornire un servizio di analisi continua delle vulnerabilità (Continuous Vulnerability Assessment) dell'infrastruttura ICT, finalizzato all'individuazione tempestiva di vulnerabilità di sicurezza, configurazioni non conformi e software obsoleto presenti su sistemi informativi, dispositivi di rete, server ed endpoint.
Il servizio dovrà essere erogato tramite piattaforma dedicata in grado di effettuare

scansioni automatiche, ricorrenti e on-demand dell'infrastruttura interna e dei sistemi esposti verso l'esterno.
La soluzione dovrà garantire almeno le seguenti funzionalità minime:

- Scansione automatizzata e continua delle vulnerabilità su sistemi, endpoint, dispositivi di rete e servizi IT.
- Individuazione di vulnerabilità note, configurazioni non sicure, patch mancanti e software non aggiornato.
- Classificazione e prioritizzazione delle vulnerabilità secondo standard riconosciuti (es. CVE, CVSS o equivalenti).
- Dashboard centralizzata per la visualizzazione dello stato di sicurezza e delle vulnerabilità rilevate.
- Reportistica periodica e on-demand, comprensiva di indicazioni tecniche per la mitigazione e la remediation.
- Notifiche automatiche in presenza di vulnerabilità critiche o ad alto rischio.
- Monitoraggio dello stato di risoluzione delle vulnerabilità e verifica della loro effettiva mitigazione.

Il servizio dovrà garantire aggiornamento continuo del database delle vulnerabilità e la disponibilità di report utili per attività di audit, gestione del rischio e miglioramento del livello complessivo di sicurezza dell'infrastruttura ICT.

5.2.5 ASSE_PATCH - Gestione patching dei dispositivi

L'aggiudicatario, avvalendosi degli strumenti di cui al punto 5.2.4 e 5.2.3, dovrà fornire al servizio ICT del comune un report mensile sullo stato di sicurezza e sulla postura dell'ente, segnalando le vulnerabilità con la relativa classificazione. Oltre a questo report l'aggiudicatario dovrà fornire un piano di rientro delle vulnerabilità classificato in base alla priorità e uno strumento che permetta al service desk dell'ente il delivery e l'applicazione di aggiornamenti e patch in maniera automatizzata su tutte le postazioni di lavoro.

5.2.6 ASSE_SOS – Servizio di sostituzione in emergenza

Fondo a consumo per interventi urgenti, sostituzioni e acquisti di apparati di rete (plafond)

La Stazione Appaltante prevede un importo massimo pari a € 10.000,00 (diecimila/00) oltre IVA, quale fondo a consumo destinato a consentire all'aggiudicatario l'esecuzione di acquisti, forniture e sostituzioni di apparati di rete o altro materiale di corredo alla rete necessari per:

- interventi in emergenza per ripristino di funzionalità e continuità del servizio;
- sostituzione di componenti guasti o non riparabili;
- sostituzione di apparati per obsolescenza tecnologica, indisponibilità sul mercato o cessazione del supporto da parte del produttore (EoL/EoS).
- materiale a corredo per la protezione o la gestione in sicurezza degli apparati (es. armadi, serrature armadi, patch cable, ausili per il cablaggio ordinato,…)

Tale importo costituisce plafond massimo spendibile e non costituisce obbligo di spesa per la Stazione Appaltante, che si riserva di utilizzarlo in tutto o in parte, senza che l'aggiudicatario possa avanzare pretese per mancato utilizzo.

Modalità di attivazione

L'utilizzo del fondo è consentito esclusivamente previa autorizzazione scritta del Responsabile del Procedimento/Direttore dell'Esecuzione del Contratto (DEC), rilasciata a seguito di richiesta motivata dell'aggiudicatario, contenente almeno:

- descrizione del guasto o della necessità di intervento;
- apparato/parte da sostituire e motivazione tecnica;
- proposta di fornitura (marca/modello o caratteristiche minime equivalenti);
- tempi di approvvigionamento e installazione;
- costo stimato e documentazione economica (preventivo/listino).

In caso di urgenza indifferibile per garantire la continuità del servizio, l'aggiudicatario potrà procedere all'intervento immediato, fermo restando l'obbligo di comunicazione entro 24 ore e convalida formale da parte della Stazione Appaltante entro i successivi 5 giorni lavorativi.

Regole economiche e determinazione dei prezzi

Gli acquisti e le forniture effettuati a valere sul fondo saranno remunerati:

- sulla base del prezzo di acquisto documentato (fattura del distributore/fornitore) oppure secondo listino concordato;
- includendo nel prezzo, se previsto, le attività accessorie di installazione, configurazione e collaudo, secondo le tariffe/condizioni del contratto.

Non sono ammesse maggiorazioni non giustificate (es. ricarichi generici), salvo spese documentate e autorizzate.

Caratteristiche tecniche dei materiali forniti

Gli apparati forniti dovranno essere:

- nuovi di fabbrica (salvo diversa autorizzazione scritta);
- originali e coperti da garanzia del produttore;
- compatibili con l'infrastruttura esistente e conformi alle normative vigenti (marchiatura CE e requisiti di sicurezza).

Sono ammesse forniture "equivalenti" o migliorative rispetto a quelle in uso, previo assenso della Stazione Appaltante.

Rendicontazione e fatturazione

Ogni utilizzo del fondo dovrà essere rendicontato tramite report di intervento, contenente:

- data e ora dell'intervento;

- descrizione dell'attività svolta;
- apparati installati/sostituiti con serial number;
- documentazione di acquisto (fatture, DDT, preventivi);
- esito del collaudo o verifica funzionale.

La fatturazione sarà effettuata a consuntivo, con evidenza separata delle spese imputate al fondo e relativo importo residuo.

Gestione del residuo

Il fondo a consumo è valido per la durata contrattuale (due anni) e si intende utilizzabile fino al raggiungimento dell'importo massimo di € 10.000,00 oltre IVA. Eventuali somme non utilizzate alla scadenza contrattuale non saranno riconosciute e non potranno essere oggetto di compensazione.

In caso di rinnovo contrattuale varranno le stesse condizioni.

5.3 MON - Servizi di Monitoraggio

L'aggiudicatario deve predisporre dei servizi di monitoraggio e fornire l'accesso o gli accessi al Direttore dell'Esecuzione del Contratto o altro referente del Comune in modo che ci sia evidenza degli incidenti rilevati e delle azioni intraprese.

In particolare i servizi di monitoraggio dovrà comprendere il NOC e il SOC

5.3.1 MON_NOC - Network Operations Center

Il servizio NOC (Network Operations Center) finalizzato al monitoraggio, alla gestione operativa e al mantenimento della continuità di esercizio dei servizi di rete.

Il servizio dovrà garantire il monitoraggio continuo dell'infrastruttura, con rilevazione tempestiva di anomalie, guasti o degradi delle prestazioni su dispositivi di rete.

Il servizio dovrà includere almeno le seguenti funzionalità:

- Monitoraggio proattivo e continuativo dello stato di funzionamento di apparati di rete, sistemi e servizi IT.
- Rilevazione automatica di malfunzionamenti, interruzioni o degradi di prestazioni.
- Gestione e presa in carico degli alert, con apertura e gestione dei ticket di incidente.
- Intervento operativo per la risoluzione o mitigazione dei problemi, anche mediante escalation verso i livelli tecnici competenti.
- Reportistica periodica sullo stato dei servizi, sugli incidenti gestiti e sui livelli di disponibilità dell'infrastruttura.

Il servizio dovrà essere erogato tramite piattaforma di monitoraggio centralizzata e garantire adeguati livelli di tracciabilità degli eventi, gestione degli incidenti e supporto alla continuità operativa dei servizi ICT.

5.3.2 MON_SOC - Security Operations Center

Il servizio deve prevedere l'interpretazione dei dati in tutte le casistiche legate alle emergenze: gestione di incidenti di sicurezza o di evento di sicurezza correlati ad allarmi da sistemi specifici o a sistemi di gestione delle minacce, di rilevamento delle intrusioni, attività di mitigazione e remediation; le attività e i sottoservizi del SOC sono dettagliati nel seguente modo:

- **Servizi di gestione:** tutte le attività di gestione delle funzionalità di sicurezza legate all'infrastruttura IT (rete, sistemi ed applicazioni);
- **Servizi di monitoraggio:** l'infrastruttura IT e di Sicurezza vengono monitorate in tempo reale al fine di individuare tempestivamente tentativi di intrusione, di attacco o di minacce reali dei sistemi e le conseguenti comunicazioni tempestive al Direttore dell'Esecuzione del Contratto o altro referente del Comune tramite e-mail e, in caso di priorità molto alta, anche tramite telefono, inerenti ogni anomalia verificatasi durante l'esercizio.
- **Servizi proattivi:** finalizzati a migliorare il livello di protezione dell'organizzazione (Security assessments, vulnerability assessments, early warning, security awareness).

Il soc dovrà anche essere in grado di dare evidenza dei login completati e falliti sui dispositivi di rete (pc, notebook, switch, firewall, ap, server) ed ove possibile servizi cloud.

5.4 SP - Servizi Professionali

5.4.1 SP_POLC - Servizio di gestione policy e configurazioni

L'aggiudicatario deve garantire le seguenti attività:

- gestione della configurazione degli apparati di sicurezza ed eventuali modifiche alle Policy, alle VPN e alle configurazioni necessarie per l'adeguato funzionamento dell'infrastruttura di rete sia in merito alla sicurezza che all'adozione di nuovi servizi che il comune potrà attivare. Non esiste un numero limite di interventi di gestione né per Policy né per VPN;
- fornire l'accesso al Direttore dell'Esecuzione del Contratto o altro referente del Comune ad un portale dedicato alla gestione delle Policy e delle VPN;
- definizione del processo di implementazione delle regole e della relativa documentazione. Tracciatura delle attività svolte secondo il processo e aggiornamento della documentazione delle regole e delle configurazioni degli apparati sotto sua manutenzione;
- l'Ente ha la possibilità di definire la priorità di creazione delle Policy secondo il seguente gradiente:
  - Creazione di Policy urgente: entro 5 ore
  - Creazione di Policy non urgente: entro 5 giorni
  - Disponibilità servizio in giorni: 5 su 7

- l’Ente ha la possibilità di definire la priorità di creazione delle VPN secondo il seguente gradiente:
  - Creazione di VPN urgente: entro 24 ore
  - Creazione di VPN non urgente: entro 7 giorni
  - Disponibilità servizio in giorni: 5 su 7

5.4.2 SP_MANA - Servizi di manutenzione

L'aggiudicatario deve altresi garantire:

- il servizio di manutenzione e assistenza per tutti gli apparati sistemi UTM firewall, dei servizi correlati (Appliance e Server di management) e degli apparati di rete;
- l’attività di verifica degli aggiornamenti e la relativa installazione sugli apparati. L'aggiudicatario verifica con continuità l’esistenza di patch, fix pack, release e aggiornamento firmware rilasciate dal produttore originario che devono essere installate sulla piattaforma del Comune al fine di adeguare quest’ultima agli ultimi aggiornamenti in tema di sicurezza e funzionalità.

  L’attività di aggiornamento deve essere concordata col Direttore dell’Esecuzione del Contratto o altro referente dell’Ente;
- il servizio di help desk illimitato per la durata del contratto;
- il servizio di help desk disponibile h24, 7 giorni su 7;
- la risoluzione di problematiche che possono mettere a rischio la continuità operativa del Comune ed in generale qualsiasi attività atta a garantire la continuità operativa in seguito al verificarsi di situazioni anomale o ad incidenti informatici, sempre in accordo con il referente del Comune e nel rispetto degli SLA rappresentati all' Art. 6 o dei loro miglioramenti in caso di offerta migliorativa dell'aggiudicatario;
- attività sistemistica di installazione e configurazione di nuovi apparati, in caso di sostituzione degli apparati specificati nell’oggetto del contratto;
- una gestione della numerosità degli incidenti illimitata.

5.4.3 SP_STRA - Servizi di supporto strategico alle decisioni su networking e cyber security

L'aggiudicatario deve garantire un servizio professionale in grado di guidare il Comune nelle decisioni in merito al networking e alla sicurezza informatica e supportare il personale del Comune nella gestione di eventi particolarmente complessi.

Si tratta di un servizio di consulenza specializzata che non va confusa con il normale supporto informativo che deve accompagnare le notifiche degli eventi derivanti dal monitoraggio. Alcuni casi tipici dove può essere richiesta la consulenza specializzata sono la fase di indagine e di raccolta di dati (“Forensic analisys”), a seguito di incidenti informatici che richiedano l’attivazione di procedure legali, oppure la fase di chiusura dell’incidente, quando si rende necessario valutare implementazioni correttive od

innovative alle difese esistenti, in grado di ridurre la possibilità che lo stesso tipo di attacco si ripeta. Altro esempio di competenza è relativo alle azioni da intraprendere a seguito delle risultanze degli assessment o alla progettazione/riprogettazione di parte della rete lan o del sistema (es. nuova sede, progettualita specifiche, cambi architetturali,…).

L'aggiudicatario deve poter erogare il servizio di consulenza specializzata secondo le seguenti modalità, in funzione dei canali di erogazione chiesti dal Comune:

- ore di consulenza "da remoto", mediante chiamata telefonica o in videoconferenza. Il servizio di consulenza "da remoto" verrà richiesto dal Comune all'aggiudicatario con apposita richiesta telefonica o scritta, da inviarsi tramite email, con la specifica indicazione sintetica del motivo per il quale viene richiesta la prestazione del servizio in parola. L'aggiudicatario si impegna a mettere a disposizione le proprie risorse per l'effettuazione di tale servizio entro e non oltre il termine di 2 giorni lavorativi a decorrere dalla predetta richiesta.
- ore di consulenza "onsite", mediante presenza presso le sedi del Comune di Cremona. Il servizio di consulenza "on site" verrà richiesto dal Comune all'aggiudicatario con apposita richiesta scritta, da inviarsi tramite email, con la specifica indicazione sintetica del motivo per il quale viene richiesta la prestazione del servizio in parola. L'aggiudicatario si impegna a mettere a disposizione le proprie risorse per l'effettuazione di tale servizio entro e non oltre il termine di 5 giorni lavorativi a decorrere dalla predetta richiesta.

L'aggiudicatario deve garantire almeno 30 ore di servizi professionali da remoto e 20 ore on-site.

L'aggiudicatario del servizio professionale deve garantire durante tutto il periodo di servizio la disponibilità di due tecnici che con continuità seguano le criticità e le progettualità dell'ente in ambito Networking e Security.

I tecnici impiegati dovranno possedere comprovate competenze in ambito networking e sicurezza informatica, attestate mediante il possesso di idonee certificazioni tecniche riconosciute a livello nazionale o internazionale.

Se nel corso dell'espletamento del servizio uno o entrambi i tecnici individuati non dovessero essere più disponibili, l'aggiudicatario deve immediatamente sostituire la/e figura/e professionale/i con altra/e paritetica/he in termini di competenze e certificazioni, a valle di comunicazione tempestiva e accettazione della sostituzione da parte della stazione appaltante.

5.5 FORM - Servizi di formazione

In fase di attivazione del servizio, l'aggiudicatario deve erogare un percorso formativo, rivolto al personale del Servizio ICT del Comune che si interfaccerà direttamente con i servizi e strumenti oggetto del presente Capitolato. Scopo del percorso formativo è abilitare detto personale ad interagire in modo efficace con le persone e gli strumenti dell'aggiudicatario. Il percorso formativo dovrà riguardare i servizi descritti al presente art. 5, quali sistema di raccolta informazioni, metodologia di monitoraggio e notifica,

comunicazione degli eventi, console, ecc. L'attività formativa potrà essere svolta online su piattaforma fornita dall'aggiudicatario.

Art. 6 Modalità di erogazione e SLA security

Ad integrazione di quanto già previsto nei precedenti articoli, si precisano di seguito ulteriori elementi necessari alla completa definizione delle prestazioni richieste.

Il servizio deve garantire la manutenzione correttiva e includere tutte le attività di coordinamento ai fini della sostituzione e di ripristino necessarie a rimuovere le anomalie riscontrate sull'impianto, per tutti i servizi descritti nel presente Capitolato prestazionale, durante le ispezioni periodiche ovvero su segnalazione del Comune, con l'obiettivo di ristabilire gli standard di qualità.

- **Tempo di presa in carico (TPC) dell'anomalia:** è l'intervallo di tempo che intercorre tra l'apertura della chiamata e l'inizio delle attività di gestione del problema;
- **Tempo massimo di ripristino in caso di failure hardware (TMR):** è l'intervallo di tempo che intercorre tra la presa in carico del problema e il ripristino del servizio in caso di guasto hardware.
- **Criticità 1 (Alta):** guasti che provocano perdita totale del servizio;
- **Criticità 2 (Bassa):** guasti che provocano perdita parziale del servizio (es: intermittenze di servizio), guasti che provocano un limitato degrado del servizio e segnalazioni varie che non modificano la qualità del servizio.

Il servizio deve rispettare i seguenti parametri per garantire gli SLA:

Parametro	Criticità 1	Criticità
Tempo di presa in carico (TPC)	4 ore	8 ore
Tempo massimo di ripristino in caso di failure hardware (TMR)	8 ore	24 ore

Il processo di gestione degli interventi deve avvenire secondo le seguenti caratteristiche minime:

- Apertura chiamate (telefonicamente, con ticket, con e-mail) deve essere garantita 24 ore su 24 per 365 giorni l'anno.
- La lingua utilizzata per tutte le comunicazioni relative alla procedura di acquisto e per quelle relative alla fornitura di tutti i servizi richiesti è la lingua italiana.
- Oltre all'italiano, si ammette l'uso della lingua inglese per le informazioni di dettaglio tecnico associate agli elementi informativi (interfaccia utente del prodotto di consultazione, comunicazioni e report tecnici, manuali, documentazione) scambiati in fase di erogazione del servizio.

Il capitolato definisce standard minimi generali (Criticità 1 e 2) con tempi di ripristino tra le 8 e le 24 ore. Tuttavia, per il servizio NOC vengono specificati parametri più stringenti di presa in carico entro 1 ora. Questa apparente differenza è coerente con la natura critica dei guasti di rete, che richiedono un'attenzione immediata per non paralizzare l'operatività dell'ente.

Art. 7 Modalità organizzative e gestione

7.1 Account Manager – Responsabile del Contratto

Prima della stipula del contratto la ditta aggiudicataria dovrà individuare ed indicare la figura professionale denominata Account Manager o Responsabile del Contratto, cui verrà affidato il coordinamento di tutte le attività inerenti il contratto e le attività inerenti la fornitura del servizio stesso (con indicazione di recapito, indirizzo mail e telefono cellulare in caso di comunicazioni e reperibilità negli orari d'ufficio dell'ente).

Tale figura dovrà:

- Capire i bisogni del cliente e proporre nuove soluzioni o prodotti
- Negoziare contratti e offerte
- Fare da punto di contatto principale tra azienda e cliente

7.2 Service Manager – Responsabile della Gestione Operativa del Servizio

La ditta aggiudicataria dovrà individuare ed indicare la figura professionale denominata Service Manager o Responsabile della Gestione Operativa, cui verrà affidata la gestione operativa del servizio (con indicazione di recapito, indirizzo mail e telefono cellulare in caso di comunicazioni e reperibilità negli orari d'ufficio dell'ente).

Tale figura dovrà:

- Garantire che il servizio funzioni correttamente
- Monitorare SLA (livelli di servizio)
- Coordinare team tecnici o di supporto
- Gestire incidenti, problemi e miglioramenti del servizio
- Assicurare la soddisfazione operativa del cliente

7.3 Comitato Tecnico

In accordo con l'aggiudicatario, entro una settimana dall'aggiudicazione definitiva, dovrà essere costituito un Comitato Tecnico (CT) per la supervisione delle attività connesse alla fornitura. Il CT sarà coordinato dal Responsabile del procedimento del Comune o suo delegato.

Tale Comitato sarà composto dall'Account Manager e dal Service Manager (potrebbe essere anche una stessa persona che svolge entrambe le funzioni) ed eventualmente da tecnici aggiuntivi dell'aggiudicatario e da personale del Comune a partire dal Responsabile dell'esecuzione del contratto e del Responsabile della Sicurezza Informatica.

Il CT esercita, nei confronti dell'Amministrazione, una funzione consultiva e propositiva in ordine all'attività di ampliamento e/o innovazione dell'intero sistema (connettività, rete) nonché di controllo con particolare attenzione alle criticità e ad eventuali incidenti. L'aggiudicatario dovrà dare evidenza negli incontri del CT dell'andamento dei servizi svolti attraverso la produzione di report mensili e materiale statistico idonei alla valutazione dell'efficacia del servizio. La tipologia del materiale statistico e dei report potrà variare a seconda delle valutazioni del CT.

Il CT si riunirà in via ordinaria con cadenza di norma bimestrale e redigerà un verbale contenente: situazione del sistema, incident report, variazioni eseguite e/o futuri ampliamenti.

E' prevista la possibilità di convocazione straordinaria in caso di criticità urgenti.

7.4 Presa in carico

L'aggiudicatario deve definire un Piano di presa in carico del servizio dall'aggiudicazione definitiva e prima della stipula del contratto.

Il Piano di presa in carico deve specificare le attività per assicurare il regolare funzionamento dell'infrastruttura e dei servizi richiesti alla data di avvio del servizio, dettagliando date e durata delle attività, modalità di esecuzione dei test, modalità di effettuazione del collaudo, necessità di supporto da parte del fornitore uscente, necessità di condivisione di documentazione, matrice delle responsabilità (chi fa che cosa e in che tempi – personale del fornitore uscente, personale dell'aggiudicatario, altri).

7.5 Tutele in uscita e lock-in

Al termine del contratto, o in caso di recesso, l'aggiudicatario è tenuto a prestare la massima collaborazione con il nuovo operatore al fine di garantire la continuità operativa di tutti i servizi.

Il passaggio dovrà essere pianificato: l'aggiudicatario dovrà fornire un piano di trasferimento per le attività di passaggio di consegna di fine fornitura. Dovrà esserci un punto di riesame insieme al fornitore entrante fino a convalida del funzionamento con il nuovo fornitore.

Art. 8 Stipulazione del contratto e relative spese

La ditta che risulterà aggiudicataria si impegna a stipulare il relativo contratto entro il termine stabilito dalla comunicazione da parte dell'Ufficio competente.

Qualora la ditta non adempia agli obblighi indicati nella suddetta comunicazione, il Comune, si riserva di revocare l'aggiudicazione ponendo a carico della ditta le eventuali

ulteriori spese che dovessero affrontare per la stipulazione con altro contraente, tenendola comunque indenne delle eventuali prestazioni effettuate nel frattempo.

Tutte le spese concernenti la stipula del contratto sono a carico dell'aggiudicatario.

Art. 9 Inadempienze e penalità

Qualora fossero rilevate inadempienze rispetto a quanto previsto dal presente capitolato prestazionale e dal contratto, il Comune invierà formale diffida tramite posta elettronica certificata, con descrizione analitica e motivata delle contestazioni addebitate e con invito a conformarsi immediatamente alle prescrizioni violate.

L'aggiudicatario ha facoltà di presentare le proprie controdeduzioni scritte entro il termine stabilito dalla diffida.

Decorso infruttuosamente tale termine senza che il gestore abbia fatto pervenire le proprie osservazioni e/o controdeduzioni o nel caso in cui le giustificazioni addotte dalla ditta aggiudicataria, non fossero ritenute soddisfacenti dall'Amministrazione, si procederà ad applicare le seguenti penali:

- una penale pari ad € 600,00 per ogni giorno di ritardo rispetto all'avvio della piena operatività del servizio SEC (v 5.1) dopo n. 1 richiamo scritto, per il quale non siano pervenute o non siano state accolte le giustificazioni addotte dalla ditta aggiudicataria;
- una penale pari ad € 300,00 per ogni giorno di ritardo nella sostituzione degli apparati messi in Eol imputabile all'aggiudicatario (v. 5.1.1) dopo n. 1 richiamo scritto, per il quale non siano pervenute o non siano state accolte le giustificazioni addotte dalla ditta aggiudicataria;
- una penale pari ad € 600,00 per ogni giorno di interruzione del servizio imputabile all'aggiudicatario (v. art. 5.2, 5.4.1 e 5.4.2) dopo n. 1 richiamo scritto, per il quale non siano pervenute o non siano state accolte le giustificazioni addotte dalla ditta aggiudicataria;
- una penale pari ad € 37,50 per ogni ora di ritardo rispetto al ripristino dello status quo ante di corretto funzionamento, in caso di incidente e/o disservizio, dopo n. 1 richiamo scritto, per il quale non siano pervenute o non siano state accolte le giustificazioni addotte dalla ditta aggiudicataria;
- una penale pari ad € 600,00 per gravi violazioni delle clausole contrattuali che compromettano la regolarità del servizio, dopo n. 2 richiami scritti, per i quali non siano pervenute o non siano state accolte le giustificazioni addotte dalla ditta aggiudicataria.

L'ammontare massimo complessivo non potrà comunque superare il 10% dell'ammontare netto contrattuale. Le somme dovute a titolo di penale non sono assoggettabili ad IVA (art.15 DPR 633/72).

L'Amministrazione potrà procedere al recupero delle penali mediante trattenuta sulla garanzia definitiva, che dovrà essere immediatamente reintegrata. Verranno tollerati ritardi

oltre i limiti sopra previsti solo in caso di eventi straordinari di particolare gravità e a fronte di documentata motivazione.

L'Amministrazione Comunale si riserva, comunque la facoltà, salvo quanto disposto al successivo comma, di far eseguire d'ufficio nel modo più opportuno, a spese della ditta aggiudicataria, le prestazioni necessarie per il regolare andamento del servizio ove la ditta stessa, appositamente diffidata, non ottemperi agli obblighi assunti.

Qualora si riscontrasse la persistenza di inadempimenti da parte dell'Impresa, appositamente diffidata, sarà facoltà dell'Amministrazione Comunale risolvere il contratto stipulato, oltre al recupero delle penali, con un mese di preavviso senza che la ditta stessa possa accampare pretesa alcuna e con ogni riserva per azioni di ulteriori danni, per i quali la Stazione Appaltante si avvarrà anche della cauzione versata, fermo restando la necessità che anche dopo il preavviso, il servizio venga regolarmente effettuato fino allo scadere del termine indicato.

Art. 10 Varianti introdotte dalla stazione appaltante

La stazione appaltante può introdurre variazioni al contratto nei casi previsti dall'art. 120 del D.Lgs. 36/2023 ed in particolare:

- per esigenze derivanti da sopravvenute disposizioni legislative e regolamentari (art. 120, comma 1, lett. c, sub. 1)
- per cause impreviste e imprevedibili, accertate dal responsabile del procedimento (art. 120, comma 1, lett. c, sub. 3) ;
- per l'intervenuta possibilità di utilizzare materiali, componenti e tecnologie non esistenti al momento in cui ha avuto inizio la procedura di selezione del contraente che possono determinare, senza aumento di costo, significativi miglioramenti nella qualità delle prestazioni eseguite (art. 120, comma 7, lett. b);
- a seguito di modifiche, spostamenti, aperture o soppressioni di sedi/uffici comunali.

Ove intervenga una variazione in aumento o in diminuzione delle prestazioni fino a concorrenza di un quinto del prezzo complessivo previsto dal contratto, l'aggiudicatario è tenuto ad eseguirle (art. 106 comma 12), previa sottoscrizione di un atto di sottomissione, agli stessi patti, prezzi e condizioni del contratto originario senza diritto ad alcuna indennità ad eccezione del corrispettivo relativo alle nuove prestazioni.

Nel caso invece le variazioni superino tale limite, la stazione appaltante procederà alla stipula di un contratto aggiuntivo a quello principale, previa sottoscrizione di atto e concordando i nuovi prezzi.

Inoltre, l'esecutore ha l'obbligo di eseguire tutte quelle variazioni di carattere non sostanziale, non comportanti maggiori oneri per l'esecutore e che siano ritenute opportune dalla stazione appaltante.

La Stazione Appaltante si riserva inoltre, senza obblighi in tal senso, di interpellare la ditta aggiudicataria in merito all'effettuazione di servizi relativi a nuove implementazioni delle reti in merito a sopravvenute esigenze; tali servizi potranno essere oggetto di idonea procedura negoziata.

Eventuali nuove implementazioni della rete dati e della rete per la fonia che si dovessero rendere necessarie nel tempo, verranno discusse e concordate dal Comitato Tecnico di cui all'art. 7.2 e congruamente valorizzate. La loro effettiva realizzazione avverrà a seguito della integrazione economica del contratto in essere.

Art. 11 Modalità dei pagamenti

La liquidazione avverrà a seguito di fatture trimestrali posticipate, previa verifica positiva di conformità al capitolato e di regolarità contributiva.

Art. 12 Revisione dei prezzi

E' ammessa la revisione dei corrispettivi contrattuali, come previsto dall'art. 60, commi 2, lett. b), e 4-quater, del D.Lgs n. 36/2023 - che richiama l'Allegato II.2-bis -, al verificarsi di particolari condizioni di natura oggettiva, che determinano una variazione del costo del servizio, in aumento o in diminuzione, superiore al 5% dell'importo del contratto e opera nella misura dell'80 per cento del valore eccedente la variazione del 5 per cento applicata alle prestazioni da eseguire dopo l'attivazione della clausola di revisione.

Per determinare l'anzidetta variazione, si utilizzano gli indici di cui all'art. 60, comma 3, lett. b), e comma 4-bis, del D. Lgs n. 36/2023, individuati con le modalità di cui all'art. 11, commi 1 e 4, del richiamato Allegato II.2-bis.

Non si applica il comma 2-bis dell'art. 60.

Come previsto dall'art. 13 dell'Allegato II.2-bis, si riporta di seguito l'associazione tra il CPV relativo al presente appalto e gli indici contenuti:

CPV	Descrizione CPV	Tabella	Tipo indice	Indice Istat – 1 **(classificazione *Ecoicop* per PC; classificazione *Ateco* per altri indici)**
72315000-6	Servizi di gestione e supporto di reti di trasmissione dati	D1	PPS	[k62.20.20] Attività di gestione di strutture informatiche

La Stazione appaltante valuta la sussistenza delle condizioni per l'attivazione automatica della clausola di revisione prezzi (anche in assenza di istanza di parte), come previsto dall'art. 3, commi 1 e 2, dell'Allegato II.2-bis del D.Lgs n. 36/2023, monitorando l'andamento dell'indice ISTAT con frequenza annuale.

Come indicato dall'art. 12, comma 1, dell'Allegato II.2-bis, la variazione è calcolata come differenza tra il valore dell'indice, individuato, ai sensi dell'articolo 11, al momento della rilevazione e il corrispondente valore al mese del provvedimento di aggiudicazione; in caso di sospensione o proroga dei termini di aggiudicazione nelle ipotesi di cui all'articolo 1, commi 3, 4 e 5 dell'Allegato I.3, il valore di riferimento per il calcolo della variazione è

quello relativo al mese di scadenza del termine massimo per l'aggiudicazione, come individuato dall'articolo 1, commi 1 e 2 del predetto Allegato.

Quando sussistono le condizioni per l'attivazione della clausola di revisione, la Stazione appaltante (RUP) comunica alla ditta aggiudicataria i prezzi revisionati da applicare alle prestazioni da eseguire successivamente al verificarsi della variazione che determina l'attivazione della clausola.

La ditta aggiudicataria, in caso di difformità in merito all'importo da riconoscere a titolo di revisione prezzi, deve richiedere – a mezzo posta elettronica certificata – verifica tempestiva in contraddittorio con la Stazione appaltante (RUP) e, in caso di perdurante disaccordo, ove intenda contestare l'importo revisionale, iscrivere riserva con le modalità e nei termini previsti dall'art. 7 dell'Allegato II.14 – a pena di decadenza dal diritto di fare valere, in qualunque tempo e modo, pretese relative ai fatti e alle contabilizzazioni risultanti dall'atto contabile (art. 115, comma 4, del D.Lgs. n. 36/2023).

I prezzi revisionati si applicano alle prestazioni eseguite/da eseguire successivamente all'attivazione della clausola. Quest'ultima si considera attivata a decorrere dalla ricezione, da parte della ditta aggiudicataria, della comunicazione a mezzo posta elettronica certificata con la quale la Stazione appaltante comunica i prezzi revisionati, che vengono riconosciuti a decorrere da tale momento, anche nell'ipotesi di eventuali contestazioni/riserve, e fino alla successiva attivazione della clausola.

Nella verifica propedeutica all'autorizzazione al subappalto, la Stazione appaltante accerta la presenza, nel contratto di subappalto (o nel sub-contratto), di apposita e conforme clausola di revisione prezzi.

Art. 13 Subappalto

Ai sensi dell'art. 119, comma 1, del D.Lgs. n. 36/2023, la ditta aggiudicataria esegue in proprio i servizi e le forniture compresi nel contratto. Fatto salvo quanto previsto dall'art. 120, comma 1, lettera d), del D.Lgs. n. 36/2023, la cessione del contratto è nulla. È altresì nullo l'accordo con cui a terzi sia affidata l'integrale esecuzione delle prestazioni appaltate, nonché la prevalente esecuzione delle lavorazioni relative alla categoria prevalente e dei contratti ad alta intensità di manodopera. È ammesso il subappalto secondo le disposizioni dell'art. 119 del D.Lgs. n. 36/2023.

Ai sensi dell'art. 119, comma 2, del D.Lgs. n. 36/2023, si evidenziano le prestazioni oggetto del contratto da eseguire a cura dell'aggiudicatario e come tali non subappaltabili:

- Servizi di Gestione Asset – art. 5.2
- Servizi di Monitoraggio – art. 5.3
- Servizi Professionali – art. 5.4

Tali limitazioni è strettamente legata alle competenze richieste ed è dettata dalla necessità di potersi interfacciare con un unico interlocutore per i servizi indicati.

La ditta aggiudicataria, prima dell'inizio della prestazione, deve comunicare alla Stazione appaltante tutti i sub-contratti che non sono subappalti, stipulati per l'esecuzione

dell'appalto, il nome del sub-contraente, l'importo del sub-contratto, l'oggetto del lavoro, servizio o fornitura affidati. Devono essere altresì comunicate eventuali modifiche intervenute nel corso del sub-contratto. Infine, eventuali variazioni dell'oggetto del subappalto, così come incrementi dell'importo dello stesso, necessitano di apposita autorizzazione integrativa.

Ai sensi dell'art. 119, comma 17, del D.Lgs. n. 36/2023, per tutte le prestazioni subappaltabili oggetto del presente appalto, è vietato il subappalto "a cascata", in ragione delle specifiche caratteristiche dell'appalto e dell'esigenza, tenuto conto della natura e della complessità delle prestazioni da svolgere, di uno stretto controllo operativo e di unitarietà nell'esecuzione.

Art. 14 Cauzione definitiva

La Ditta aggiudicataria, a tutela del regolare adempimento degli obblighi contrattuali, prima della stipula del relativo contratto, sarà obbligata a costituire la garanzia definitiva nella misura e secondo le modalità di cui all'art.117 del D. Lgs. 36/2023.

Art. 15 Trattamento dei dati personali

I dati personali presenti nella documentazione prodotta dai concorrenti sono prescritti dalle disposizioni vigenti ai fini del procedimento per i quali sono richiesti e verranno utilizzati esclusivamente per tale scopo, nel rispetto delle vigenti normative in materia di trattamento dei dati personali.

L'aggiudicatario sarà nominato responsabile esterno nell'ambito del servizio e nella gestione dei dati dei servizi oggetto dell'appalto e pertanto dovrò attenersi alla normativa vigente compreso il regolamento Europeo GDPR e alle relative regole tecniche.

Art. 16 Tutela patrimonio Informativo – Tipologia di dati acceduti

I dati trattati dall'operatore economico durante il servizio di SECNaaS sono e rimangono di proprietà esclusiva del Comune di Cremona.

L'operatore economico dovrà eseguire gli interventi di assistenza senza accedere al contenuto di file ad esclusione di quelli di configurazione dei sistemi. Si esclude quindi accesso e trattamento di dati personali per l'operatore economico.

Art. 17 Norme corrispettivo

Laddove, intervenisse una convenzione Consip (o di un'altra centrale di committenza regionale aggregata) migliorativa delle condizioni contrattuali, e qualora l'appaltatore non acconsenta ad una modifica delle condizioni economiche tali da rispettare i parametri Consip, l'Amministrazione potrà recedere in qualsiasi momento dal contratto ai sensi dell'art. 1 comma 13 del D.L. n. 95/2012 come convertito dalla Legge n.135/2012.

Art. 18 Risoluzione del contratto

Il Comune di Cremona si riserva la facoltà di risolvere il contratto nei termini e con le modalità previste dall'art. 122 del D. Lgs. n. 36/2023.

Costituiscono cause di risoluzione di diritto del contratto, ai sensi dell'art. 1456 c.c., previa formale contestazione degli addebiti e assegnazione di un termine di 10 giorni per le controdeduzioni, le seguenti ipotesi di grave inadempimento dell'aggiudicatario:

- se nel giorno fissato e comunicato, l'aggiudicatario non dà avvio al servizio così come indicato all'art. 2 del presente Capitolato;

- interruzione o sospensione ingiustificata del servizio per un periodo superiore a 5 giorni lavorativi complessivi, anche non consecutivi;

- reiterata inosservanza delle prescrizioni organizzative e operative impartite dal Responsabile unico del progetto tale da compromettere la regolare esecuzione del servizio;

- superamento dell'ammontare complessivo delle penali nella misura massima del 10 per cento dell'importo contrattuale;

- violazione degli obblighi in materia di tracciabilità dei flussi finanziari;

- perdita dei requisiti di ordine generale o speciale richiesti per l'affidamento;

- grave violazione degli obblighi di riservatezza o trattamento dei dati personali;

- subappalto non autorizzato o cessione del contratto in violazione della normativa vigente;

- mancato rispetto delle disposizioni in materia di sicurezza sul lavoro tale da determinare pericolo per persone o beni;

- ottenimento per due volte consecutive del Durc negativo;

- il contraente venga diffidato due volte, con nota scritta, circa la mancata puntuale esecuzione della prestazione nel rispetto dei termini contrattuali;

- nel caso dovessero permanere le condizioni che hanno portato all'addebito di anche una sola delle penali previste dal presente Capitolato;

3. Resta ferma la facoltà della stazione appaltante di procedere alla risoluzione del contratto anche al di fuori delle ipotesi sopra tipizzate, nei casi previsti dalla normativa vigente in materia di contratti pubblici.

Art. 19 Recesso

L'Amministrazione Comunale si riserva la facoltà di recedere dal contratto in applicazione all'art. 123 del D. Lgs. 36/2023.

Art. 20 Cessione del contratto

È vietata la cessione, totale o parziale, del contratto. Ogni atto contrario è nullo.

Art. 21 Controversie

Qualsiasi controversia in merito all'interpretazione, esecuzione, validità o efficacia del contratto tra l'Amministrazione Aggiudicatrice e l'Aggiudicatario saranno demandate al giudice ordinario. Foro competente è il Tribunale di Cremona.

Art. 22 Norme finali

La partecipazione alla gara comporta la piena ed incondizionata accettazione di tutte le disposizioni del presente Capitolato, del bando e del disciplinare di gara.

Per tutto quanto non previsto specificamente nei documenti su citati, si fa espresso riferimento a quanto previsto in materia dalla vigente normativa comunitaria e nazionale, per quanto compatibile.