ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296 – **LOTTO 1**

PIANO DEI FABBISOGNI

NOTA BENE:

Durante l'esecuzione contrattuale è possibile che il progresso tecnologico innovi i servizi di base con l'introduzione di nuove funzionalità e/o nuovi servizi in ogni caso complementari/supplementari ai servizi previsti in gara mediante procedura negoziata ai sensi dell'art. 63 co. 3 lett b), d.lgs. n. 50/2016 oppure mediante una modifica ai sensi dell'art. 106 co.1 lett. b) d.lgs. n. 50/2016.

L'organismo tecnico di Coordinamento e Controllo, raccolta la necessità di introduzione di un nuovo servizio, esclusivamente se lo stesso risulta nella disponibilità dell'aggiudicatario dell'Accordo Quadro, richiederà allo stesso, sulla base di un apposito documento di "specifiche tecniche" (con annessi i requisiti da garantire), la quotazione di un servizio da inserire nei servizi oggetto di fornitura. Tale nuovo servizio sarà dunque inserito in perimetro tra i servizi acquistabili.

INDICE

1. DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione:	Comune di Firenze
Indirizzo	Piazza della Signoria, 1
CAP	50122
Comune	Firenze
Provincia	FI
Regione	Toscana
Codice Fiscale	01307110484
Codice IPA	c_d612
Indirizzo mail	direzione.sistemiinformativi@comune.fi.it
PEC	direzione.sistemiinformativi@pec.comune.fi.it

Referente Amministrazione	Luca Bertelli
Ruolo	Dirigente Tecnico
Telefono	055 3283813 - +39 329 5603051
Indirizzo mail	luca.bertelli@comune.fi.it
PEC	direzione.sistemiinformativi@pec.comune.fi.it

2. CONTESTO

- ***DESCRIZIONE DELL'AMMINISTRAZIONE CONTRAENTE***

Inserire una breve descrizione dell'Amministrazione contraente e del suo compito istituzionale.

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

Firenze è un comune italiano di circa 380.000 residenti, capoluogo dell'omonima provincia della Toscana, ottavo comune italiano per popolazione e primo della regione Toscana.
Il presente progetto è attivato e governato dalla Direzione Sistemi informativi (in seguito DSI) del Comune di Firenze.

La DSI, è stata protagonista nell'ultimo trentennio di tutta l'innovazione tecnologica del Comune di Firenze, partendo dal centro elaborazione dati basato su mainframe, avviando nei vari uffici dell'ente le prime sperimentazioni di office automation, realizzando in proprio numerosi gestionali, e poi via via evolvendo le infrastrutture e le tecnologie utilizzate al passo con la rapidissima crescita che è propria del settore ICT (Information & Communication Technology).
La DSI opera contemporaneamente su due fronti. Da un lato nei confronti di migliaia di dipendenti che devono essere messi in grado di poter lavorare in modo efficace ed efficiente, e di migliaia di cittadini che devono ricevere servizi dai sistemi IT gestiti; dall'altro, è chiamata a porsi come soggetto promotore di innovazione, di sperimentazione di soluzioni di nuova generazione (cloud computing, mobile computing, open government, cybersecurity), e di stimolo alla digitalizzazione dell'intera Amministrazione e della città stessa.

I due fronti fanno riferimento sia all'inquadramento normativo che regolamenta la cosiddetta Pubblica Amministrazione Digitale e il Piano Triennale per l'Informatica nella Pubblica Amministrazione, sia al continuo confronto con altre realtà metropolitane italiane ed europee. L'obiettivo di fondo è sempre quello di far sì che i cittadini di Firenze, le aziende, i professionisti ed i turisti possano beneficiare di servizi digitali all'avanguardia, caratterizzati da un'offerta sempre più usabile, confrontabile con le più avanzate esperienze nazionali ed estere, e che gli stessi vengano erogati in piena sicurezza. La sicurezza informatica è pertanto ormai un aspetto imprescindibile, che deve permeare qualsiasi sistema informativo e assicurarne costantemente le classiche proprietà di riservatezza, integrità e disponibilità.

- ***DESCRIZIONE DEL CONTESTO TECNOLOGICO, APPLICATIVO E PROCEDURALE***

Inserire la descrizione del contesto tecnologico ed applicativo (anche eventualmente mediante apposito allegato) al fine di permettere al Fornitore la declinazione nel Piano Operativo delle specifiche esigenze.

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

La DSI ha poi la responsabilità e la gestione diretta di circa 70 apparati fisici IT (blade, host, firewall, appliance, storage NAS e SAN, fiber channel switch, etc.) tra quelli ospitati presso il data center di Regione Toscana; nella vecchia sala server, ad oggi sala dedicata alla connettività e ad ospitare apparati di sistemi secondari, presso la sede della DSI; e infine nella saletta per i backup e parziale DR presso la sede della Protezione Civile comunale. In questo caso, l'evoluzione tecnologica ha giocato un ruolo fondamentale in quanto, praticamente, la totalità dei server applicativi è ormai virtualizzata e si contano

diverse centinaia di virtual machine (vm), quindi è stato intrapreso da tempo quel percorso di consolidamento e di ottimizzazione delle risorse ICT indispensabile, e al tempo stesso abilitante, verso l'adozione di future soluzioni di cloud computing. Infatti, è stato avviato da tempo ed è in corso di conslusione il processo di migrazione dell'intera infrastruttura virtualizzata del Comune in un ambiente di "private cloud", secondo il paradigma IaaS (Infrastructure-as-a-Service), nel Sistema Cloud Toscana (SCT), cioè l'ambiente cloud predisposto da Regione Toscana per gli Enti aderenti alla convenzione.

Il sistema informatico centralizzato fornisce oltre 2.500 servizi informatici, tra quelli di base e di alto livello, che coprono tutti gli ambiti dell'infrastruttura ICT interna (sistemi operativi, middleware, dbms, application e web server, software e proxy applicativi, programmi, web services, apps, etc.), e garantisce giornalmente elevati livelli di disponibilità, di interoperabilità, di accessibilità e di fruibilità del dato, tipici di un moderno sistema informativo basato sulla qualità della gestione dell'informazione, aspetto al quale è indispensabile collegare anche adeguati livelli di monitoraggio e controllo in ambito sicurezza informativa. Del resto, la DSI impiega una molteplicità di tecnologie per la fornitura dei servizi ed è stata già introdotta la complessità dell'attuale sistema informatico esistente nell'Ente e della dimensione del bacino di utenza, interno ed esterno, a cui sono rivolti centinaia di servizi in esso ospitati. L'obiettivo di garantire elevati livelli di disponibilità, di interoperabilità, di accessibilità, di fruibilità, di integrità e di riservatezza (ove richiesto) del dato si scontra, di fatto, con questa molteplicità di servizi, varietà di utenti e numerosità dei sistemi IT che è necessario governare al meglio; quindi, con gli impatti che questo comporta in ambito sicurezza informatica.

Entriamo adesso nel dettaglio del contesto di riferimento per questo progetto.

Sul versante di rete, per gli uffici viene utilizzata la rete metropolitana in fibra ottica proprietaria del Comune (FI-Net), con apparati hardware dedicati (router, switch, hot-spot wifi) e relativi sistemi di gestione della sicurezza (quali regole di controllo dell'accesso – ACL, reti private virtuali – VPN, sicurezza tramite firewall). Rientra in questo contesto anche la realizzazione di una vasta connettività WiFi, in continua e costante espansione, nelle aree strategiche del territorio comunale per erogare connettività agli utenti finali.

Sul versante sistemistico e servizi ICT di base si può segnalare che:

- vengono impiegate tecnologie di virtualizzazione dei server da diversi anni, tanto che ormai oltre il 95% del sistema informativo elettronico è ospitato ed erogato sfruttando questo sistema;
- sono attivi oltre 330 server e appliance Linux-based e oltre 120 server Windows;
- è in funzione una soluzione principale di virtualizzazione per ospitare tutte le vm dell'Ente ed è tale struttura fisica che verrà progressivamente dismessa a favore del passaggio nell'ambiente IaaS già citato,
- sono presenti alcuni storage minori di memorizzazione dati per diverse centinaia di TB, altri con funzioni residuali di copie dei backup o di archiviazione dati digitali per una quantità pari sempre a centinaia di TB di dati;
- è attivo un sistema centralizzato di backup e parziale disaster recovery (DR) che mantiene oltre un centinaio di TB di dati salvati su storage dedicato e altre centinaia di TB di copie storiche in uno storage di "archive" in diversa sede, con una produzione giornaliera di diversi TB di salvataggi di dati aggiornati;
- si utilizzano sistemi operativi e middleware, sia proprietari sia open source per combinare al meglio i pregi, le best practices e i punti di forza delle due realtà;
- sono adottate più tecnologie DBMS (in particolare Oracle EE, Postgres, MySQL, MariaDB, Microsoft SQL): produttori diversi per rispondere al meglio alla specificità dei diversi software, alle esigenze di ogni applicativo, alle valutazioni costi-benefici o ai vincoli dei progetti da realizzare;
- è stata ultimata la migrazione delle caselle di posta personali e di quelle condivise di ufficio verso l'ambiente collaborativo online costituito dalla soluzione in cloud Microsoft Office 365, su tenant della tipologia business per gli uffici ordinari e su tenant educational per tutto il personale afferente alla Direzione Istruzione;
- i servizi centralizzati di dominio, di posta elettronica, di navigazione web e di antivirus sono realizzati per circa 3.700 postazioni client mediante un'infrastruttura combinata e interconnessa di appliance, alcuni server fisici e numerosi virtuali,

realizzati mediante software open source (proxy o gateway di navigazione, gateway di posta elettronica e relativi sistemi di protezione e filtraggio) e a licenza per assicurare una elevata disponibilità e piena sicurezza al relativo servizio.

Sul versante software e applicativi sono utilizzati strumenti di programmazione e sviluppo avanzati (RAD – Rapid Application Development), framework che soddisfano il paradigma IT di livello enterprise e sistemi automatici condivisi di gestione delle versioni dei sorgenti (CVS - Concurrent Versioning System) in modo da realizzare applicazioni che rispondano alle esigenze prospettate dagli uffici committenti e utilizzatori. In tale ambito è opportuno precisare che sono gestite sia applicazioni sviluppate con risorse interne, sia applicazioni acquisite sul mercato, a loro volta distinte tra pacchetti off the shelf (per es. produttività di ufficio) e applicazioni del tutto personalizzate (per esempio gestione documentale, gestione del personale). Da alcuni anni è stato implementato un repository centralizzato con a bordo Git, uno strumento molto potente che permette la conservazione il tracciamento delle versioni del software sia di front end, sia di quello realizzato internamente per i progetti aziendali. Le applicazioni sviluppate con risorse interne sono realizzate utilizzando una piattaforma creata all'interno dell'Ente, pubblicata anche su GitHub nazionale, basata su varie componenti open source, costantemente aggiornata da un punto di vista delle versioni delle componenti software, della sostituzione di eventuali obsolescenze, di applicazione di nuovi schemi progettuali, sottoposta costantemente a verifica di sicurezza. Le applicazioni sviluppate internamente soddisfano le richieste delle Direzioni committenti, sia di automazione di ufficio che di carattere generale trasversale (esempio: valutazioni delle performance del personale), ma gestiscono anche servizi rivolti alla cittadinanza.

Dal punto di vista dei gestionali esterni, vi è un'attenta e continua attività che ha come obiettivo anche il miglioramento dei servizi offerti ai cittadini, grazie sia all'adeguamento normativo che a quello tecnologico. A tal proposito, sono in corso attività per la sostituzione di importanti sistemi informatici quali, ad esempio il sistema di gestione delle Pratiche edilizie e ambiente (PEA), vari gestionali di front e di back office, gli sviluppi funzionali necessari ai vari back office per completare e/o ottimizzare l'integrazione con la piattaforma abilitante PagoPA, ecc.

Analogamente, sono in corso di completamento le attività di sviluppo di nuovi progetti, come quello di dematerializzazione delle pratiche e vengono erogati numerosi servizi online multipiattaforma.

Una peculiarità della Direzione Sistemi Informativi consiste nel fatto che il Sistema Informativo Territoriale (SIT), che spesso nelle organizzazioni è un ufficio a parte, è incardinato nella Direzione; infatti, considerato che il dato viene individuato come elemento centrale per l'organizzazione, è stato costituito un ufficio della DSI che si occupa di dati a 360 gradi, quindi non solo dei dati georeferenziati su mappe digitali, dei sistemi di Business Intelligence e di raccolta e analisi dei Big Data e sentiment analysis, ma che, più in generale, è orientato ad una grande attenzione al fenomeno della metadatazione, catalogazione e della data governance, in modo da promuovere la cultura del dato e da poter fornire sempre il miglior supporto decisionale. Molto importante anche la fornitura di dati in modalità open: il portale open data dell'ente è, dal 2011, molto attivo e mette a disposizione come dati pubblici strati informativi molto raffinati, oltre all'annuario statistico.

Il front end on line del Comune è costituito dal sito web istituzionale (detto anche Rete Civica), dai siti web tematici e da diversi moduli on line che consentono la sottomissione di semplici istanze da parte dei cittadini. Utilizza un CMS (Content Management System) come ambiente di sviluppo, che si appoggia a un'infrastruttura ridondata collocata all'interno dei sistemi dell'Ente, ed è gestito direttamente dalla Direzione Sistemi Informativi. La pubblicazione dei contenuti che quotidianamente vengono generati sui siti web avviene nel rispetto di un'organizzazione ormai consolidata negli anni, che coinvolge circa un centinaio di redattori appartenenti alle diverse Direzioni del Comune, coordinate per gli aspetti redazionali dall'Ufficio comunicazione e per quelli tecnici dalla Direzione Sistemi Informativi.

Sono parte integrante del front end on line del Comune di Firenze i Servizi On Line (detti anche SOL), ovvero lo strumento attraverso il quale numerose categorie di cittadini (es.: genitori, famiglie, professionisti, operatori economici, ecc.) hanno la possibilità di interagire per via telematica con l'Ente, attraverso un canale sicuro ed efficace.

In generale, per ciascuno dei servizi sopra descritti, viene assicurato controllo e supervisione, supporto informatico e un servizio di help desk multilivello.

▪ DESCRIZIONE DELL'ESIGENZA

Contestualizzare l'oggetto della richiesta in riferimento all'attuale quadro dell'Amministrazione specificando eventuali misure e azioni intraprese per l'avvio di progetti finalizzati alla trasformazione digitale dei propri servizi in base al Modello strategico evolutivo dell'informatica della PA e ai principi afferenti al Piano Triennale per l'informatica della Pubblica Amministrazione.

Il presente capitolo ha lo scopo di descrivere le esigenze del Comune di Firenze nell'ambito dei servizi offerti dall'Accordo quadro AQ 2296 – Lotto 1 per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, stipulato da Consip S.p.A. (Consip) e dal Raggruppamento Temporaneo di Imprese (RTI) composto da:

- Accenture S.p.A.
- Fastweb S.p.A.
- Fincantieri NexTech S.p.A.
- Difesa e Analisi Sistemi S.p.A.

Per incrementare il livello generale di sicurezza informatica del proprio sistema informativo, come già indicato nel precedente paragrafo, il Comune di Firenze ha deciso di ricorrere al presente accordo quadro necessario per il mantenimento di una serie di servizi mirati in ambito cybersecurity per coprire ambiti e rispondere a particolari esigenze e necessità, in questo momento gestite e adeguatamente trattate solo fino al 31 dicembre 2023. Con questo intervento, il Comune di Firenze si pone pertanto l'obiettivo di confermare una buona capacità di fronteggiare un attacco cyber in tutte le sue fasi, garantendo un livello generale di resilienza del proprio sistema ICT anche negli ambiti non presidiati direttamente - sia a causa della mancanza di strumenti tecnologici sia per carenza di personale con conoscenze specialistiche necessarie - ma ad oggi realizzati tramite i servizi del presente AQ, seppur previsti fino alla data già indicata.

Tale mantenimento delle capacità di monitoraggio continuo degli eventi e di risposta agli incidenti di sicurezza ha come obiettivi la riduzione del tempo di rilevazione di un'anomalia/incidente, la riduzione del tempo di reazione per il contenimento dell'attacco, l'eradicazione del problema, il ripristino rapido delle funzioni eventualmente compromesse e la reportistica relativa all'evento. Per garantire al meglio questi obiettivi è necessario *disporre* di tecnologie che consentano la raccolta e la correlazione continua di una grande mole di informazioni provenienti da una telemetria pervasiva di utenti/dispositivi/applicazioni, *avvalersi* delle competenze di elevata specializzazione che sappiano utilizzare questi strumenti, *agire* in caso di incidente in stretta collaborazione tra l'outsourcer e le strutture dell'Amministrazione preposte alla gestione sistemistica (IT Operation).

L'intervento prevede l'acquisizione delle funzionalità di SOC evoluto, quindi il loro mantenimento fino al 31 dicembre 2024 in quanto servizi già in essere - supportate dall'infrastruttura necessaria all'implementazione della Protezione degli Endpoint con monitoraggio continuo degli eventi di sicurezza (agent EDR) e alla abilitazione delle funzioni di correlazione (piattaforma di threat intelligence, strumento di log collection p.e. SIEM) - degli eventuali servizi di configurazione e tuning delle policy, dei servizi di supporto all'analisi e alla pianificazione delle attività. Il servizio deve prevedere la generazione di una reportistica da condividersi con l'Amministrazione con cadenza periodica concordata che potrà essere utilizzata per pianificare azioni di miglioramento continuo della security posture.

Il Comune di Firenze si impegna ad effettuare l'opportuna segnalazione al Centro di Valutazione e Certificazione Nazionale (CVCN) qualora i servizi richiesti siano inseriti nel Perimetro di sicurezza nazionale cibernetica.

▪ *SINTESI DEI SERVIZI RICHIESTI*

Le richieste del presente Piano dei Fabbisogni riguardano l'erogazione (il mantenimento) dei seguenti servizi con le metriche/fasce di servizio adeguate in base a quanto effettivamente rilevato nel corso del 2023:

- **Servizio "Protezione end-point"**

Il servizio indicato dovrà consentire alla DSI di proteggere i dispositivi collegati alla rete aziendale del Comune di Firenze dall'accesso non autorizzato o dall'esecuzione di software dannoso. La protezione degli endpoint deve garantire, inoltre, che i dispositivi raggiungano un livello di sicurezza definito e siano conformi alle policy e ai requisiti di conformità e sicurezza stabiliti dal Comune di Firenze. Nel dettaglio devono essere fornite le funzioni di: protezione con sistemi antimalware; ispezione localmente del traffico HTTPS; controllo dell'uso o anche blocco dei dispositivi USB; trasmissione degli eventi alle piattaforme di correlazione (nel rispetto della normativa privacy); monitoraggio continuo delle minacce avanzate e protezione da malware basati su file e senza file; protezione e prevenzione dalla perdita di dati.

- **Servizio "Security Operation Center (SOC)"**

  Si richiede di mantenere, attraverso gli adeguati strumenti tecnologici di back-end, un servizio di monitoraggio e alerting degli eventi/minacce di sicurezza al fine di consentire una gestione degli incidenti di sicurezza dalla fase di identificazione e notifica dell'evento, fino alle azioni di contenimento, ripristino e prevenzione futura in stretta collaborazione tra l'outsourcer e le strutture dell'Amministrazione preposte alla gestione sistemistica. Tra le funzioni richieste ci si aspetta quindi raccolta centralizzata dei log e degli eventi; correlazione tra eventi diversi raccolti; disponibilità di un cruscotto (dashboard) che fornisca agli analisti, in tempo reale, una rappresentazione della situazione in essere; capacità di identificazione, gestione, mitigazione e risoluzione degli attacchi; produzione di report periodici di sintesi, di incident report di dettaglio ed istruzioni operative. Si richiede, infine, di ricevere ed analizzare la reportistica e i log dando anche la giusta priorità ai processi di risoluzione e/o mitigazione delle minacce.

- **Servizio "Gestione continua delle vulnerabilità di sicurezza**"

  Si richiede di implementare un servizio remoto che dovrà consentire, al personale della DSI, tramite un processo automatico di assesment delle vulnerabilità, di ottenere una fotografia precisa del livello e gravità del rischio a cui, in quel momento, sono esposti i propri sistemi informatici. Il servizio si avvarrà dell'utilizzo di uno scanner che produrrà un report con le specifiche indicazioni di rischio relative alle vulnerabilità rilevate. Tra le funzioni richieste si prevede la capacità di completa scansione nella complessa infrastruttura del Comune di Firenze (come descritta nei precedenti paragrafi); capacità di individuare i livelli di gravità e classificazione CVSS; possibilità di disporre di un report; attività a supporto per la risoluzione o mitigazione di quanto rilevato.

- **Servizio "Threat intelligence e Vulnerability data feed"**

  Il servizio richiesto dovrà consentire al personale della DSI individuato, di ricevere un flusso continuo o, almeno, periodico a scadenze concordate di dati relativi a minacce e vulnerabilità di sicurezza del sistema informativo del Comune di Firenze o che coinvolga in qualche modo asset, account e/o credenziali afferenti al Comune. Devono essere disponibili le informazioni più recenti, permettendo così di prevedere/prevenire le minacce prima che entrino in azione migliorando gli attuali controlli e le funzionalità di protezione già presenti.

- **Servizi specialisti**

  Si richiede di prevedere un'adeguata quantità di ore per ingaggiare specialistici e team di cybersecurity per dare supporto, gestire, trattare o comunque coprire quanto già dettagliato nei precedenti servizi e nei paragrafi di descrizione del contesto di interesse.

Tali servizi sono riassunti nella seguente tabella che descrive le numerosità richieste per la loro erogazione. Si richiede, altresì che il piano di lavoro abbia una **durata complessiva di 12 mesi, da 01/01/2024 fino a 31/12/2024**.

L1.S1 – SECURITY OPERATION CENTER								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno (2 mesi)**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S1	Security Operation Center		A canone (annuale)	Fino a 300 Eps				
				Fino a 600 Eps	601			

		As a service (Device equivalenti)		Fino a 1.200 Eps				
				Fino a 6.000 Eps				
				> 6.000 Eps				

L1.S4 – GESTIONE CONTINUA DELLE VULNERABILITÀ								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno (2 mesi)**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S4	Gestione continua delle vulnerabilità	As a service	A canone (canone annuale per indirizzo IP)	Fino a 50 IP				
				Fino a 200 IP				
				> 200 IP	1.000			

L1.S5 – THREAT INTELLIGENCE & VULNERABILITY DATA FEED								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno (2 mesi)**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S5	Threat intelligence & Vulnerability data feed	As a service	A canone (canone annuale per datafeed)	Fino a 10 datafeed				
				Fino a 50 datafeed	30			
				> 50 datafeed				

L1.S7 – PROTEZIONE END POINT								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno (2 mesi)**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S7	Protezione End Point	As a service	A canone (canone annuale per numero di nodi)	Fino a 500 nodi				
				Fino a 1.000 nodi				
				Fino a 5.000 nodi	4.150			
				> 5.000 nodi				

L1.S15 – SERVIZI SPECIALISTICI								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S15	Servizi specialistici	A task	A corpo	gg/p Team ottimale	525			

Nell'ambito dei servizi richiesti, si elencano di seguito i servizi per i quali è richiesto il collaudo:

- L1.S1 Security Operation Center
- L1.S4 Gestione continua delle vulnerabilità
- L1.S5 Threat intelligence & Vulnerability data feed
- L1.S7 Protezione End Point
- L1.S15 Servizi Specialistici

  - ***LUOGO DI EROGAZIONE***

In base alla modalità di esecuzione dei servizi le prestazioni contrattuali dovranno essere svolte come di seguito indicato:

- per i servizi erogati *da remoto*: presso i Centri Servizi del Fornitore;
- per i servizi *on-site*: presso le sedi principali di interesse del Comune di Firenze per il proprio sistema ICT, quindi principalmente nella sede della Direzione Sistemi Informativi in via Reginaldo Giuliani 250 (FI), eventualmente anche presso la sede della Protezione Civile in via dell'Olmatello 25 (FI) o anche presso la sede del datacenter regionale TIX in via San Pietro a Quaracchi, 250 (FI).

INDICATORE DI PROGRESSO

Per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID, ove successivamente modificate ed integrate, sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura (acquisto di servizi previsti nell'Ordinativo), che sarà determinato come da schema seguente:

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

LUCA
BERTELLI
Comune di
Firenze
19.09.2023
08:56:54
GMT+01:00