PROCEDURA APERTA PER L'ACQUISIZIONE DI SERVIZI DI IT SYSTEM MANAGEMENT E SICUREZZA INFORMATICA 2

CAPITOLATO TECNICO

LOTTI 1 e 2

ALLEGATO 3

(RETTIFICATO)

INDICE

1. PREMESSA

Il presente Capitolato Tecnico disciplina gli aspetti tecnici della Convenzione per la fornitura di servizi relativi all'IT System Management e alla Sicurezza Informatica per le Pubbliche Amministrazioni della Regione Emilia-Romagna (seconda edizione).

2. OGGETTO DELL'ACQUISIZIONE

L'oggetto della fornitura si compone di due lotti: il Lotto 1 riguarda i servizi di gestione, manutenzione, sviluppo delle architetture informatiche e supporto specialistico per le infrastrutture hardware e software di base utilizzati dalle Amministrazioni della Regione Emilia-Romagna a supporto delle proprie attività informatizzate (IT System Management); il Lotto 2 riguarda i servizi necessari e funzionali a garantire adeguati livelli di sicurezza dei sistemi IT nel loro complesso, dei dati trattati e in generale delle informazioni (Sicurezza Informatica).

Il complesso dei servizi e delle attività ricomprese nei due lotti è quindi volto a garantire la piena operatività delle infrastrutture tecnologiche, a mantenerne la perfetta efficienza, a garantire agli utenti la disponibilità e le prestazioni delle applicazioni su di esse installate, l'integrità e confidenzialità dei relativi dati, nonché a fornire il supporto necessario per garantirne il costante allineamento con l'evoluzione tecnologica del mercato ICT e delle soluzioni e servizi di Sicurezza Informatica e a definirne la crescita in coerenza con gli obiettivi strategici delle Amministrazioni stesse.

Si sottolinea che i contesti tecnologici e le architetture applicative sono da intendersi come una fotografia di un panorama tecnologico che è in continua e rapida evoluzione. Pertanto, le Ditte concorrenti dovranno sapersi adeguare in modo flessibile al mutare del contesto di riferimento e dovranno cogliere le opportunità fornite dall'evoluzione tecnologica per proporle ed implementarle, ove necessario, nel sistema informatico delle Amministrazioni.

Oltre al contesto tecnologico si deve tenere conto anche dell'evoluzione normativa nazionale ed europea in materia di Data Protection e Cybersecurity.

Sempre più importante è la costante formazione del personale e delle terze parti delle Amministrazioni, la conoscenza e il know-how tecnico aziendale sul tema della sicurezza informatica, Security Awareness and Training, in aderenza agli standard ISO/IEC 27001, ai Framework nazionale e internazionale (NIST) per la Cybersecurity e la Data Protection e in coerenza con il GDPR (Regolamento europeo 679/2016).

Di seguito si descrivono le caratteristiche tecniche dei servizi richiesti.

3. CONTESTO TECNOLOGICO DELLA FORNITURA

L'ambito tecnologico nel quale dovranno essere erogati i servizi previsti comprende le principali tecnologie presenti nel mercato dell'ICT e della Sicurezza Informatica, ampiamente utilizzate dalle Pubbliche Amministrazioni. Di seguito viene fornita, a titolo puramente indicativo e non esaustivo, una panoramica degli ambiti tecnologici in questione.

3.1 Distribuzione delle infrastrutture

Le infrastrutture hardware e software di base utilizzate da ciascuna Amministrazione possono essere concentrate in un'unica sede o possono essere suddivise su più sedi distribuite sul territorio.

In linea generale, ove il sistema informativo abbia una struttura distribuita su più sedi, i diversi datacenter sono collegati tra loro mediante rete geografica; inoltre, il sistema informativo nel suo complesso dispone tipicamente di collegamenti alla rete internet e al Sistema Pubblico di Connettività (SPC).

Sono da tenere presenti gli sviluppi normativi nazionali per cui la distribuzione potrebbe evolvere secondo quanto previsto per il Polo Strategico Nazionale (PSN), con le conseguenti attività di adeguamento.

3.2 Tipologie hardware e software

Ciascuna Amministrazione può disporre di apparecchiature hardware e prodotti software di base e specifici di varia tipologia, specializzati per diversi ambiti progettuali e funzionali. Nella tabella seguente si riporta una sintesi delle varie tecnologie e dei principali produttori/prodotti presenti sul mercato ICT. Si sottolinea che tale elenco è fornito a puro titolo indicativo e non esaustivo.

Il Fornitore prende atto che le Amministrazioni possono introdurre variazioni dell'ambito tecnologico a fronte di specifiche esigenze delle Amministrazioni stesse, o per le naturali evoluzioni dei sistemi ICT e necessità di adeguamento dei livelli di sicurezza e si impegna ad erogare i servizi di system management o sicurezza informatica adeguando le conoscenze del personale impiegato o inserendo nei gruppi di lavoro risorse con skill adeguato, senza alcun onere aggiuntivo per le Amministrazioni.

Sistemi Operativi e Tecnologie di Virtualizzazione	
Sistemi Operativi	Linux (Red Hat, CentOS, Ubuntu, FreeBSD, Debian, Suse, Oracle), Windows, Apple Mac OSX
Software di virtualizzazione	VMware, Hyper-V, Citrix, RHeV
Software di Infrastruttura	

Storage management	SAN management software, HSM (Brocade DCFM, CA Technologies SRM, EMC Ionix ECC, Hitachi Storage Command Suite, HP Storage Essentials, IBM TPC, NetApp OnCommand)
Backup & recovery	CA Technologies ArcServer, CommVault Simpana, EMC Data protection suite, HP DataProtector, IBM TSM, Symantec Netbackup
Application integration & middleware software	integration middleware (web services, ESB, message-oriented middleware) (IBM Websphere MQ, Oracle Fusion middleware, RedHat Jboss ESB, Software AG WebMethods, Tibco)
	application server & transaction processing (Apache Tomcat, IBM Websphere, Microsoft .NET framework, Oracle Weblogic, RedHat Jboss)
	portals and web infrastructure (IBM Websphere portal, Microsoft Sharepoint, OpenText, Oracle Webcenter portal, RedHat Jboss EPP, Docker e Kubernetes)
Data management and integration	database management systems and tools (administration, utilities, monitoring) (DB2, Oracle, SQL Server, MySQL, PostGresSQL, MongoDB)
	data integration (ETL, quality, metadata) (IBM Infosphere, Informatica Powercenter, Microsoft SSIS, Oracle, SAP, SAS Dataflux)
Enterprise content management	Document management, Workflow/Business Process Management, Web content management (Alfresco, Microsoft Sharepoint, IBM FileNet e Webcontent manager, Oracle Webcenter, OpenCMS, OpenText)
IT operations management software	System monitoring (Microsoft Operations Manager, Oracle Enterprise Manager, IBM Tivoli, BMC, CA, HP)
	Security agent (antivirus, activity monitor & audit solution, logging)
	Application performance monitoring (BMC, CA, Compuware, HP, Oracle, Quest Software)
	IT service management (service desk, asset, change, configuration management) (BMC Remedy, CA Service Desk Manager, IBM Smartcloud Control Desk) workload automation (BMC Control M, CA workload automation, IBM Tivoli workload scheduler)
Identity & data management software	Identity and access management (single sign-on), Data access management (FAM), Privileged access management (PAM)
Enterprise Software	
Business Intelligence	IBM Cognos, Microstrategy, Oracle BIEE, Pentaho, Qlicktech, SAP BusinessObjects e BW
Customer Relationship Management	Oracle Siebel, SAP Customer Service
Enterprise Resource Planning	SAP/R3, SAP HANA, SAP BPC, SAP HR ed eRecruiting, Oracle JD

	Edwards EnterpriseOne, SAGE ERP X3
Api Management	Kong API Gateway and Service Connectivity Platform, Wso2
Software Client	
Client software	sistemi operativi client e dispositivi mobili (Windows, Apple, Android)
	prodotti software di informatica individuale (MS Office, MS SharePoint, OpenOffice)
	web browser (MS Edge, Firefox, Chrome, Safari)
	antivirus (MCAfee, Norton, Trend Micro ecc.), data leak prevention ed encryption
	Sistemi di virtualizzazione (XenApp, XenDesktop)
	software distribution e remote desktop control
Tecnologie Hardware	
Server	server entry-level, midrange o enterprise, configurazioni standalone, rack o blade, architettura x86 o RISC
Storage	SAN, NAS, protocolli fiber channel, fiber channel-over-Ethernet, iSCSI, Infiniband, tape library e virtual tape library, object storage
Network & security	Protocolli di rete e di routing per reti locali, cablaggio strutturato, sistemi wireless, apparati (switch, router, firewall, load balancer, wifi access points), network solutions (Alcatel-Lucent, Avaya, Brocade, Check Point software, Cisco, Extreme Networks, Fortinet, HP)
Tecnologie Data Analytics	
Big data/Data Analytics	Apache Spark, Kafka, Hadoop, Ambari, Redash e Azure Synapse
Tecnologie Cloud	
Public Cloud	Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)
Tecnologie Sicurezza	
Security software, technology and service	Data security (encryption), endpoint, server e email security (antivirus, antimalware, anti-ransomware), xDR Detection and Response, network security (firewall, VPN, IDS/IPS) e Network Access Control (Forescout, Fortinac), Data Loss Prevention (DLP), Zero Trust Architecture, Penetration Test e Vulnerability assessment su sistemi e reti (LAN e Wifi), Vulnerability management e Web Application Scan, DAST, SAST, SCA: verifica del codice dinamico e statico per applicazioni sicure nell'intero ciclo di vita (SDLC a garanzia del principio generale di "sicurezza e privacy by design e by default"). Risk management.
Monitoring and orchestrator	Security information and event management – SIEM e Security Orchestration, Automation and Response - SOAR (Microsoft Sentinel

	IBM, MICROFOCUS, Splunk, ecc…) UEBA (User and Entity Behavior Analytics)
Threat intelligence and information sharing	External Attack Surface Management (EASM), Threat Intelligence service e Commercial Digital Risk Protection, MISP Threat Sharing
Security Awareness	Piattaforme specialistiche di ambito E-Learning training and gaming

4. CARATTERISTICHE, MODALITA' E SPECIFICHE DEI SERVIZI

Di seguito sono descritti in dettaglio i servizi richiesti per il Lotto 1 "IT System Management" e il Lotto 2 "Sicurezza Informatica" oggetto della Convenzione.

4.1 Lotto 1 – IT System Management

Il presente Lotto 1 annovera al suo interno un insieme di servizi e attività che in virtù della loro complessità e soprattutto criticità devono essere svolti in piena e stretta sinergia con le figure professionali dell'IT, interno all'Ente, del Fornitore dei servizi di Sicurezza Informatica o di eventuali altre figure professionali che operano per conto dell'Amministrazione. Per questo è richiesta la massima collaborazione fra le parti, in accordo con l'Amministrazione committente.

Di seguito l'elenco dei Servizi inerenti al presente Lotto.

4.1.1 Servizi di Monitoraggio Sistemi e Reti

Il "Servizio di Monitoraggio Sistemi e Reti" comprende al suo interno il servizio di monitoraggio operato sullo strato network dell'architettura, erogato dal **NOC – Network Operation Center.**

In particolare, il sottoservizio **NOC** si occuperà della rilevazione di malfunzionamenti hardware e/o software tali da rendere irraggiungibili od inutilizzabili i servizi effettuando gli interventi di primo livello e le attività di escalation verso i livelli superiori a seguito di procedure schedulate.

Pertanto, il Fornitore deve disporre all'interno del proprio Centro Servizi per l'Operatività da Remoto del servizio NOC da mettere a disposizione delle Amministrazioni che facciano richiesta di servizi da erogare mediante tale modalità operativa.

La lingua di riferimento per l'erogazione dei servizi deve essere l'italiano.

Da tale Centro, attraverso l'utilizzo degli opportuni strumenti e mediante l'impiego di personale specializzato, il Fornitore dovrà avere la possibilità di operare in collegamento con i sistemi dell'Amministrazione per effettuare tutte le attività di gestione che non richiedono necessariamente la presenza di personale in loco, ad esempio:

- monitoraggio dei sistemi, delle reti, delle applicazioni e dei database;
- gestione dei processi di service management;

- esecuzione dei processi di change semplici e proceduralizzati (definizione utenze, reset password, ecc.);
- attività di Gestione Operativa remotizzabili (riavvio application server, ecc..).

Compreso inoltre:

- controllare costantemente (sulla base delle finestre di erogazione del Servizio concordate con l'Amministrazione) il sistema di "monitoraggio ed allarmistica" per poter intervenire proattivamente e/o tempestivamente in caso di attivazione di regole di allarme o superamento di soglie critiche preimpostate su tutti i componenti della rete compresi tutti i server dell'infrastruttura;
- ricevere, qualificare e gestire fino a chiusura le richieste di assistenza che potranno generarsi da tale sistema di monitoraggio o tramite chiamata sia di personale dell'Amministrazione, sia di Help-desk di società terze che forniscono servizi di manutenzione su sistemi hardware e software utilizzati dall'Amministrazione stessa;
- gestire in autonomia la gestione degli allarmi, contattando servizi di Help-Desk di fornitori terzi (quali provider di connettività, manutentori di sistemi hardware e software, etc.), contattando il personale tecnico dell'Amministrazione qualora ve ne sia la necessità; l'Amministrazione fornirà al Fornitore l'elenco dei numeri utili ed i relativi codici di accesso per i vari Helpdesk qualora presenti.
- essere un single point of contact attivo e raggiungibile (sulla base delle finestre di erogazione del Servizio concordate con l'Amministrazione) tramite numero di telefono ed e-mail;
- coordinare gli interventi on-site di fornitori terzi e se necessario prendere i relativi accordi logistici con le strutture presso le quali gli apparati sono installati. La Ditta dovrà collaborare con il fornitore terzo fino al completo ripristino della configurazione e la ripresa delle complete funzionalità;
- provvedere ad inviare periodicamente (con cadenza concordata con il personale dell'Amministrazione), tramite comunicazione e-mail, un riepilogo degli allarmi attivi e di tutte le criticità in atto;
- informare il personale dell'Amministrazione di eventuali anomalie/guasti, all'insorgere dell'allarme;
- generare report relativi a target monitorati; periodicità e tipologia dei report generati verranno concordati con l'Amministrazione.

Da parte del NOC dovrà essere realizzato un accesso ridondato al sistema di monitoraggio installato presso l'Amministrazione, in modo da garantirne l'utilizzo anche in caso di fault del collegamento primario.

Tutto il personale del NOC deve essere in grado di prendere in carico tutte le attività relative all'infrastruttura dell'Amministrazione, al fine di garantire una continuità di servizio al Committente; a tal fine, pertanto, il Fornitore deve adeguatamente formare ed istruire il personale del NOC, relativamente all'infrastruttura ICT dell'Amministrazione stessa.

Il NOC del Fornitore deve rispettare inoltre le seguenti regole:

- la connessione telematica tra il Centro Servizi e le sedi dell'Amministrazione deve essere realizzata attraverso canale dedicato punto-punto a costo del Fornitore. Nessun onere potrà essere ascritto all'Amministrazione. Si intende ricompresa nella connessione anche la dotazione degli apparati di networking ed ogni altra dotazione necessaria, inclusi i cablaggi dalla terminazione di rete del Provider del collegamento ai locali CED dell'Amministrazione. La soluzione deve garantire adeguate prestazioni e affidabilità in caso di malfunzionamento di uno dei componenti dell'infrastruttura;
- il Fornitore deve predisporre presso il proprio Centro servizi una soluzione tecnologica, avente prestazioni e affidabilità adeguate anche in caso di malfunzionamento di uno dei componenti dell'infrastruttura, atta a garantire ai gruppi impegnati nell'erogazione dei servizi;
- In particolare:

  a) **Un punto di accesso alla rete dell'Amministrazione** ed eventualmente, su richiesta, anche un punto di accesso dedicato al sito di Disaster Recovery. In particolare, il Fornitore dovrà garantire che gli accessi alla rete ed ai sistemi dell'Amministrazione avvengano esclusivamente dal personale identificato mediante utenze nominative autorizzate dal proprio sistema di gestione degli accessi. Per quanto riguarda l'accesso ai sistemi di proprietà dell'Amministrazione, il Fornitore dovrà utilizzare utenze nominative nelle modalità concordate con l'Amministrazione, compatibilmente alle specifiche tecnologie e sempre in conformità con quanto previsto dal provvedimento del Garante in materia di accesso degli amministratori di sistema. Non è richiesta la realizzazione di un sistema di Single Sign On che consenta l'uso delle medesime credenziali nei due domini (Sistemi del Centro servizi e Sistemi dell'Amministrazione);

b) **Autenticazione e profilazione delle utenze**. Il processo di autenticazione e profilazione delle utenze è riferito al punto di accesso alla rete dell'Amministrazione;

c) **Tracciatura degli accessi ai sistemi** (login, ssh, desktop remoto, ecc.). In ottemperanza al provvedimento del Garante per la protezione dei dati personali, in materia di accessi degli amministratori di sistema, dovrà essere possibile registrare gli accessi e le attività eseguite dagli amministratori, sul sistema per la gestione degli accessi del Centro Servizi. Per quanto riguarda la registrazione degli accessi e delle attività degli Amministratori su ciascun sistema di proprietà dell'Amministrazione, le modalità saranno concordate con l'Amministrazione;

d) **Conservazione dei Log**. È richiesta la conservazione per almeno un anno dei log del sistema di gestione degli accessi, utilizzato per l'accesso alla rete ed ai sistemi dell'Amministrazione, utilizzando strumenti di conservazione e di gestione dei log predisposti dal Centro servizi del Fornitore. L'Amministrazione si riserva di richiedere tali log con frequenza periodica in base alle procedure concordate con il Fornitore stesso.

- il Fornitore deve garantire la sicurezza del collegamento e la riservatezza dei sistemi e delle informazioni attraverso la formalizzazione e l'applicazione di procedure e politiche di sicurezza da adottare al proprio interno, adeguate ai requisiti stabiliti. Infatti, è responsabilità del Fornitore assicurare che il Centro Servizi, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni da e verso la rete dell'Amministrazione siano protette mediante l'adozione di adeguati sistemi e metodologie definite utilizzando come riferimento le norme della serie ISO/IEC 27001. In particolare, nell'esecuzione dei servizi, il Fornitore deve garantire l'evoluzione, la manutenzione e l'adeguamento tecnologico dei sistemi, delle reti e di tutti gli strumenti impiegati presso il Centro servizi che si rendano necessarie a soddisfare i requisiti di sicurezza stabiliti, nonché l'aggiornamento delle politiche di sicurezza e delle contromisure attuate e la risoluzione reattiva o proattiva di incidenti di sicurezza.

In considerazione dell'esigenza di garantire il massimo grado di copertura di tutti gli aspetti di sicurezza, si richiede la redazione di un Piano della Sicurezza, in conformità a best practice e/o a standard internazionali, secondo quanto concordato con l'Amministrazione.

Nel seguito si riportano alcuni requisiti da intendersi come minimi.

Categoria	Requisiti minimi

Sicurezza delle reti	Il punto di accesso alla rete dell'Amministrazione deve essere adeguatamente protetto mediante sistemi firewall che operino secondo modalità note come "Stateful inspection". Devono essere utilizzati sistemi/meccanismi di intrusion detection e prevention che analizzino il traffico in entrata ed in uscita dalla rete dell'Amministrazione.
Riservatezza dei dati e delle trasmissioni	Deve essere garantita la riservatezza di tutti i dati gestiti.
Integrità dei dati	Devono essere adottati antivirus centralizzati ad aggiornamento periodico, che analizzino e bonifichino gli eventuali codici malevoli. Devono essere adottati antivirus su tutte le postazioni utilizzate dal personale del Fornitore e collegate con la rete dell'Amministrazione. Tali postazioni devono soddisfare lo standard per le postazioni di lavoro previste per l'Amministrazione
Auditing e vulnerability assessment	Devono essere registrati tutti gli eventi telematici che hanno impatto sui sistemi, effettuati dal Centro servizi del Fornitore, permettendo la ricostruzione di comportamenti insidiosi e l'individuazione di possibili responsabilità penali e civili conseguenti condotte illecite. Tali registrazioni dovranno essere effettuate e conservate sui sistemi del centro servizi che consentiranno l'accesso alla rete dell'Amministrazione, ovvero sui sistemi dell'Amministrazione, secondo le modalità concordate con l'Amministrazione.
Amministrazione accessi	Devono essere adottati adeguati processi di Amministrazione degli accessi (fisici e logici) effettuati nel Centro servizi che prevedano l'identificazione delle diverse categorie di utenti, la definizione dei corrispondenti profili di autorizzazione e delle modalità di rilascio dell'accesso.

Il Fornitore deve garantire la continuità dei servizi anche in caso di evento disastroso e/o di interruzione della connessione tra il Centro servizi e la rete dell'Amministrazione.

In particolare, il Fornitore deve implementare una soluzione, tecnica ed organizzativa, che consenta di garantire il ripristino delle funzionalità al fine di garantire l'erogazione dei servizi ed il rispetto dei requisiti di qualità contrattuali.

Il Fornitore, se richiesto dall'Amministrazione, dovrà mettere a disposizione una piattaforma di Monitoraggio dei sistemi e delle applicazioni (diversamente utilizzerà la piattaforma già in essere presso l'Amministrazione committente).

La piattaforma di monitoraggio dovrà consentire di tenere sotto controllo lo stato operativo dei sistemi e delle relative componenti e degli apparati di rete, rilevando automaticamente informazioni quali a titolo esemplificativo, ma non esaustivo, le seguenti:

- Stato dei diversi sistemi, sottosistemi, servizi ed apparati;
- Parametri critici per la funzionalità dei diversi sistemi, sottosistemi, servizi ed apparati, definendo dei valori di soglia che denuncino la prossimità di situazioni critiche. Ad esempio, per i server tali parametri potranno riguardare: Spazio Disco, Utilizzo memoria, utilizzo CPU, utilizzo schede di rete;
- Stato dei processi applicativi che siano di particolare rilevanza per la funzionalità dei servizi erogati.

Gli eventi generati dalla piattaforma di monitoraggio dovranno essere collezionati in appositi Log. La piattaforma dovrà inoltre essere configurata in modo da intraprendere eventuali azioni correttive in maniera automatica.

Nell'ambito della piattaforma di monitoraggio, il Fornitore dovrà prevedere una soluzione per il monitoraggio end-to-end dei servizi applicativi erogati agli utenti finali, in modo da poterne facilmente verificare lo stato operativo e prestazionale.

Correlando tutte le informazioni provenienti dai vari sistemi che costituiscono l'ambiente di esercizio con quelle relative alle transazioni applicative, la soluzione dovrà dare evidenza dello stato operativo dei servizi applicativi erogati ed essere così di supporto alla rapida risoluzione dei problemi.

In particolare, dovrà consentire di identificare automaticamente le componenti da controllare lungo la catena applicativa in caso di errore.

Oltre a monitorare la disponibilità dei servizi applicativi e ad essere di supporto nella risoluzione dei problemi, la soluzione dovrà consentire di verificare e controllare le performance dei servizi erogati per verificarne l'aderenza ai livelli di servizio attesi.

Il software di monitoraggio fornito dal Fornitore (se richiesto dall'Amministrazione) dovrà essere installato su server di proprietà dell'Amministrazione stessa.

Compito del Fornitore sarà in particolare di:

- installare la piattaforma di monitoring e tutti i software necessari al suo corretto funzionamento sui server dell'Amministrazione; tutti i software necessari al funzionamento del monitoraggio non dovranno avere alcun costo di licenza aggiuntivo (compreso il sistema

operativo dei server);

- provvedere alla configurazione di target monitorabili tramite SNMP, script sviluppati su misura, verifica di URL, query sui principali DB (Oracle, MySQL, SQLServer, ecc…), verifiche su file di log, sviluppo di moduli aggiuntivi per soddisfare le esigenze puntuali;
- assistere il personale dell'Amministrazione nella definizione ed ottimizzazione dei target da monitorare;
- permettere l'accesso al portale WEB di monitoraggio tramite autenticazione Active Directory o LDAP (diversi domini di autenticazione potranno esistere contemporaneamente);
- profilare gli accessi al sistema di monitoraggio.

4.1.2 Servizi di Conduzione Operativa Sistemi

La "Conduzione Operativa Sistemi" comprende sia i servizi base di gestione continuativa (sottoservizio "**Server logici e fisici"**) sia i servizi di gestione delle piattaforme di memorizzazione e archiviazione (sottoservizio "**Storage/Backup"**). La conduzione dei sistemi "**Server logici e fisici"** prevede quindi la manutenzione attiva dei sistemi, la gestione dei software di base e d'ambiente, le basi dati, la gestione sicurezza logica di base e la gestione della configurazione nonché delle variazioni dovute a normale conduzione degli apparati precedentemente citati. È compito del servizio di conduzione dei server, secondo le specifiche dell'apparato in oggetto (mail server, DB server, etc.) predisporre, governare e presidiare la corretta esecuzione dei piani di backup in aderenza a quanto previsto dal piano dedicato. Per quanto attiene la gestione dei sistemi di storage e backup, attività erogata nel sottoservizio dedicato, sono comprese nel servizio la gestione delle LUN, la modifica/creazione di nuovi segmenti e aree di archiviazione, la gestione delle autorizzazioni ed abilitazioni all'accesso delle stesse aree di memorizzazione. Relativamente alla gestione dei backup rientra all'interno dei compiti del servizio la verifica della funzionalità degli apparati dedicati, il check sul corretto stato di servizio dei supporti di memorizzazione (siano essi magnetici a cassetta o HDD). Sarà compito del servizio anche la segnalazione di eventuali malfunzionamenti e/o deterioramenti degli apparati laddove tali danni dovessero compromettere la funzionalità degli apparati e di conseguenza inficiare il buon esito delle politiche di backup. Si evidenzia che, gli apparati switch fibre channel, per le loro peculiari caratteristiche, risultano amministrati in questo servizio e non nella macrocategoria "Conduzione Operativa Reti".

Pertanto, per Conduzione Operativa si intende il complesso delle attività riconducibili all'ordinaria gestione e manutenzione dell'infrastruttura IT garantendone il funzionamento e l'efficienza.

Gli obiettivi della conduzione operativa sono:

- garantire la disponibilità dei sistemi e l'esecuzione delle attività schedulate;

- assicurare un continuo controllo sullo stato dei sistemi e dei collegamenti, individuare criticità o malfunzionamenti ed intraprendere le azioni necessarie;
- prevenire, gestire e risolvere tutti i problemi che comportano interruzione o degrado del servizio all'utenza;
- ottimizzare l'utilizzo dello storage in termini di razionalizzazione degli accessi e garantire la disponibilità, la salvaguardia e l'integrità dei dati;
- garantire l'efficienza dei sistemi rispetto all'utilizzo delle risorse hardware e software;
- controllare l'impatto sulla tecnologia esistente e garantire l'adeguamento degli ambienti elaborativi a fronte dell'immissione in esercizio di modifiche correttive e/o evolutive di applicazioni esistenti;
- monitorare e verificare i consumi effettivi delle eventuali infrastrutture e servizi in cloud.

Nella conduzione operativa sistemi sono incluse, a titolo indicativo, le attività descritte nei paragrafi di seguito.

4.1.2.1 Presa in carico di nuovi Servizi e Tecnologie

L'attività è finalizzata alla presa in carico di nuovi servizi, sistemi, procedure operative e di tutti gli elementi base oggetto dei servizi di gestione (sistemi, apparati HW, prodotti SW e firmware).
Il Fornitore è responsabile di effettuare tutte le attività necessarie per l'avviamento e per la presa in carico sia nei casi in cui le attività realizzative siano state effettuate dal Fornitore stesso sia nei casi in cui le attività realizzative siano state effettuate da terze parti (es. vendor).
Il Fornitore è responsabile:

- di eseguire le procedure definite dall'Amministrazione per la messa in produzione delle infrastrutture;
- di eseguire le procedure definite all'interno del processo di "Service Asset & Configuration Management" per l'identificazione dei nuovi Elementi di Configurazione;
- dell'implementazione e gestione delle politiche di software Distribution relativamente al parco tecnologico dell'Amministrazione della verifica, valutazione ed eventuale integrazione della documentazione prevista dall'Amministrazione.

4.1.2.2 Gestione Piattaforme Elaborative

Le attività sono volte a mantenere un ambiente di elaborazione stabile e tale da garantire il soddisfacimento dei requisiti operativi. Più in dettaglio, le attività consistono nell'integrazione dei prodotti di terze parti con le componenti del sistema operativo, comprendendo le attività di aggiornamento, test di funzionalità e distribuzione del software utilizzato, nel rispetto dell'evoluzione

tecnologica dei sistemi, degli standard di mercato e dei livelli di servizio contrattuali. La gestione degli ambienti elaborativi prevede in particolare:

- l'installazione, personalizzazione, distribuzione, manutenzione e test del sistema operativo, dei sottosistemi e dei prodotti del middleware (Web Server, Application Server, Data Server, ecc.);
- la definizione ed attuazione delle procedure di automazione operativa (script di avvio/arresto, controllo dei servizi, trasferimento automatico di dati, ecc.);
- le configurazioni necessarie all'integrazione di prodotti software (configurazioni dei prodotti relativi all'ambiente, alla sicurezza, alla connettività, all'autenticazione attraverso servizi di gestione centralizzata delle utenze, alla comunicazione tra diversi layer tecnologici, ad es. Application server e Data Base server);
- coordinamento degli interventi di manutenzione HW;
- verifica periodica delle fonti di pubblicazione dei bollettini di sicurezza per le tecnologie in uso presso l'Amministrazione ed esecuzione periodica dell'aggiornamento dei sistemi per la rimozione delle vulnerabilità di sicurezza (installazione patch, windows update, modifiche alla configurazione dei servizi, ecc.) in accordo con le misure di prevenzione degli incidenti definite dal committente. A tal proposito, si precisa che l'Amministrazione consentirà l'utilizzo delle utenze di accesso ai network dei vendor di cui è in possesso, con cui il Fornitore potrà consultare informazioni relative alla sicurezza. Tuttavia, il Fornitore dovrà accedere a bollettini pubblici e/o informazioni ottenute attraverso propri canali, a complemento della citata attività;
- coordinamento ed esecuzione di tutte le attività legate alla conduzione dei siti di disaster recovery/business continuity sia nella normale conduzione (compreso l'allineamento dei dati fra i vari siti ove richiesto), sia a fronte dei test periodici e a fronte di dichiarazioni di disastro da parte dell'Amministrazione. L'Amministrazione si riserva di effettuare test di DR ogni qualvolta l'evidenza della situazione, variazioni significative dell'infrastruttura, obblighi normativi o procedure di qualificazione per i servizi IT che l'Amministrazione dovrà o vorrà osservare, lo richiedano.

In generale, il Fornitore è tenuto farsi parte proattiva nel proporre e analizzare modifiche agli apparati gestiti, al fine di mantenerli allineati alle ultime fix, release e versioni del software installato.

4.1.2.3 Gestione delle Procedure Batch

Le procedure batch si articolano in:

- batch applicativo, schedulato a seguito di richiesta effettuata dalle varie aree applicative;
- batch tecnico, che riguarda essenzialmente il salvataggio dei dati e la memorizzazione dei dati di sistema, utilizzati per la produzione di report statistici mensili.

Il Fornitore ha la responsabilità del buon esito del batch tecnico per tutti i prodotti installati, compresi quelli di automazione. Inoltre, il Fornitore ha la responsabilità, a fronte di errori di esecuzione del batch applicativo, di fornire il supporto per verificare eventuali cause riconducibili all'infrastruttura. Il Fornitore si impegna ad utilizzare i prodotti messi a disposizione dall'Amministrazione per l'automazione delle attività di IT Operations in ambienti open.

4.1.2.4 Gestione Alta Affidabilità

Per tutti i sistemi per i quali sia stato configurato un meccanismo di alta affidabilità (per esempio cluster Microsoft, cluster Linux, Oracle RAC, ridondanza di connessioni fisiche), sulla base della periodicità concordata o a fronte di un change complesso su uno specifico sistema, il Fornitore deve produrre un piano che descriva le modalità di test, i risultati attesi, ed eseguire il test secondo la tempistica concordata con l'Amministrazione.

4.1.2.5 Gestione dello Storage

L'attività si sostanzia principalmente nel:

- controllare l'utilizzo dei dischi e delle Virtual Tape Library (VTL), per assicurare la disponibilità di spazio;
- gestire lo spazio sui dischi e le VTL;
- riorganizzare gli archivi, per assicurarne la massima efficienza;
- creare, gestire e ripristinare i cataloghi utente;
- classificare i tipi di dati e le applicazioni che li utilizzano;
- ottimizzare l'utilizzo dello storage;
- definire le politiche di gestione VTL4;
- l'analisi conoscitiva dell'utilizzo dello storage e produzione costante di reportistica;
- bonificare i dati obsoleti;
- la configurazione degli switch per le necessità di nuovi collegamenti (zoning, ecc.) e inizializzazione dei dischi.

Le politiche di backup da adottare sono definite dall'Amministrazione; per politiche di gestione delle VTL si intende la realizzazione delle suddette politiche di backup tramite l'implementazione e la

gestione sulle VTL, di procedure operative, configurazioni e automazioni e quant'altro il fornitore ritenga necessario.

Le politiche di backup definiscono Retention prestabilite per classi di dati e servizi; pertanto, per bonifica dei dati si intende il recupero degli spazi di archiviazione della VTL a scadenza delle singole Retention.

4.1.2.6 Backup e Restore Management

L'esecuzione delle operazioni di backup e restore è basata sui prodotti in uso presso l'Amministrazione che si interfacciano con i vari tool disponibili per ciascuna tipologia di Piattaforma/Database.

Il Fornitore deve garantire la continuità dei servizi e/o il recupero dei dati (dati di sistema e delle applicazioni) in tutti i casi in cui si renda necessario, comprendendo l'ultima transazione eseguita con successo.

Sulla base delle politiche definite dall'Amministrazione, è responsabilità del Fornitore definire la pianificazione delle attività di backup, al fine di ottimizzare la finestra temporale a disposizione.

4.1.2.7 Gestione Database

Il Fornitore deve effettuare l'amministrazione, ottimizzazione e installazione dei database ospitati dai sistemi gestiti. Le attività da svolgere nell'ambito di tale servizio sono, ad esempio, le seguenti: installazione e upgrade dei prodotti, configurazione ed amministrazione dei database, riorganizzazione dei dati.

A titolo esemplificativo ma non esaustivo si prevedono le seguenti attività:

- installazione e configurazione del database;
- DB Administration (creazione tabelle, caricamento dati, ripristino degli indici, ottimizzazione dei DB, ecc.);
- aggiornamento dati statistici del catalogo del database;
- soluzione delle anomalie;
- installazione delle fix correttive e di sicurezza;
- installazione nuovi release;
- reporting periodico per evidenziare le frammentazioni dei database;
- analisi delle prestazioni delle singole sessioni applicative ed individuazione di possibili ottimizzazioni del codice.

4.1.2.8 Gestione Dominio

Il Fornitore deve effettuare la gestione del dominio secondo le politiche definite dall'Amministrazione, in particolare per ciò che concerne la sicurezza.

Le principali attività svolte nell'ambito dell'erogazione del servizio sono le seguenti:

- gestione sistemistica dell'AD: attività di conduzione funzionale dell'Active Directory, quali il monitoraggio, il backup, il patch management (limitatamente ai domain controller) e la gestione log (raccolta ed archiviazione) per tutti i Domain Controller;
- gestione degli account utente su AD
- gestione del dominio: gestione delle policy, dei computer in dominio, della propagazione delle policy sui singoli computer, gestione del servizio DNS.

Il Fornitore deve provvedere alla sospensione/cancellazione di tutte le utenze riconducibili al Fornitore uscente, dando evidenza dell'operazione all'Amministrazione tramite elenchi ordinati per server (ordinati per dominio nel caso di utenze di dominio), entro il termine massimo concordato con l'Amministrazione in fase di subentro. Inoltre, entro tale medesimo termine, il Fornitore deve provvedere alla modifica delle password per tutte le utenze di tipo Amministrazione o Super User, secondo le politiche in essere.

4.1.2.9 Gestione Middleware

Le principali attività da svolgere nell'ambito dell'Amministrazione di tali prodotti sono:

- installazione e configurazione dei prodotti e loro evoluzione e manutenzione;
- deploy delle applicazioni e/o degli oggetti applicativi (applicazioni, report, siti, folder, ecc.);
- implementazione di configurazioni di scalabilità orizzontale o verticale (configurazione dei domini, dei cluster, dei cloni, ecc.) a seconda delle necessità;
- configurazione delle integrazioni tra i servizi (Enterprise Service Bus, Single Sign On, ecc.);
- configurazione delle code, degli End Point, ecc…;
- configurazione delle utenze e dei relativi privilegi;
- analisi dei log e delle eccezioni applicative o sistemistiche;
- analisi delle prestazioni degli specifici ambiti di installazione applicativa (ad es. Java Virtual Machine, Microsoft IIS) utilizzando gli strumenti propri di ogni singolo midlleware (Oracle Enterprise Manager, ecc.);
- correzione delle anomalie e manutenzione periodica per l'allineamento del livello di patch necessario alla rimozione dei bug e delle vulnerabilità dei prodotti;
- predisposizione di script gestionali per l'avviamento e l'arresto delle singole applicazioni o di

specifici processi/componenti;

- gestione dei componenti/device periferici (libreria ottica, stampanti di sistema, ecc.);
- predisposizione degli agent di test e di profilazione delle applicazioni e supporto all'analisi dei dati raccolti.

In considerazione della rapida evoluzione di queste tecnologie e delle frequenti opportunità di variazione del contesto tecnologico dell'Amministrazione, soprattutto per l'adozione di nuove piattaforme middleware, il Fornitore deve garantire un adeguato rinnovamento delle competenze.

4.1.2.10 Definizione delle Procedure Operative

È richiesto che il Fornitore effettui la definizione delle procedure operative a supporto della standardizzazione delle attività tecniche afferenti i servizi di Conduzione Operativa dei Sistemi dell'infrastruttura e ne produca la documentazione di dettaglio.

Inoltre, è responsabilità del Fornitore predisporre e mantenere aggiornate procedure automatiche (script, procedure, ecc.) a supporto delle attività di conduzione. Ciascuna procedura automatica è accompagnata dalla documentazione concordata, da sottoporre all'approvazione dell'Amministrazione, necessaria all'eventuale presa in carico e manutenzione della procedura stessa da parte dell'Amministrazione o da terzi da essa designati. Il formato ed i contenuti di tale documentazione sono concordati nel corso degli incontri tecnici.

Nell'eventualità in cui l'Amministrazione si avvalga di terzi per la predisposizione di procedure automatiche, il Fornitore ha la responsabilità di prendere in carico le stesse nonché di effettuarne la gestione e gli eventuali successivi adeguamenti.

L'Amministrazione si riserva la facoltà di sottoporre a verifica e/o accettazione le procedure realizzate e/o modificate dal Fornitore.

4.1.2.11 Gestione Piattaforme di Posta Elettronica

Il servizio di Conduzione Operativa Sistemi deve comprendere anche il servizio di gestione della posta elettronica che prevede: la gestione e l'aggiornamento periodico dei sistemi di posta elettronica in uso presso l'Amministrazione; la gestione dei backup, del monitoraggio degli stessi e dell'eventuale recovery dell'intero sistema server e/o della singola casella e-mail.

Obiettivo della fornitura del servizio di gestione della posta elettronica è permettere il regolare funzionamento 24h x 365 giorni/anno, salvo brevi periodi di manutenzione, della posta elettronica in ingresso ed in uscita, mediante le attività necessarie, quali (a titolo esemplificativo e non esaustivo) quelle di seguito definite:

- gestire il servizio di posta elettronica dei domini di posta, assicurando la manutenzione e il

corretto funzionamento del servizio;

- dare il necessario supporto alla corretta gestione/creazione/eliminazione degli indirizzi di posta elettronica o alias, assegnati a ciascun utente o a liste di distribuzione;
- effettuare il controllo antivirus ed anti-spamming sui sistemi coinvolti ed attivare, le eventuali azioni di contrasto;
- effettuare periodicamente il controllo del corretto funzionamento ed aggiornamento del sistema antivirus sui sistemi di posta;
- garantire adeguate misure di sicurezza al fine di evitare usi impropri dei Server che fanno parte del Sistema preposto al servizio di posta elettronica;
- garantire un efficace livello di performance del servizio ed azioni in direzione del miglioramento delle stesse;
- garantire tempi rapidi di ripristino del servizio o di ogni sua parte componente in caso di disservizio;
- apportare modifiche alle configurazioni dei sistemi di posta per allinearli con le esigenze che possono emergere;
- implementare e manutenere i meccanismi di aggiornamento/creazione automatica delle caselle di posta e di ogni altro elemento del sistema (realizzati tramite scripting per es.).

Tutte le attività di gestione ordinaria/straordinaria del sistema di posta elettronica dovranno essere preventivamente concordate con il personale dell'Amministrazione.

4.1.3 Servizi di Conduzione Operativa Reti

La **"Conduzione Operativa Reti"** prevede la manutenzione attiva dei sistemi di rete, la gestione delle regole di routing e di sezionamento delle reti (VLan). E' compresa la copia e backup delle configurazioni degli apparati in aderenza a quanto previsto dall'apposito piano, qualora esistente.

Il servizio ha la finalità di garantire il corretto funzionamento dell'infrastruttura attiva di rete LAN attraverso il suo continuo monitoraggio e l'interazione con i fornitori titolari dei contratti di manutenzione delle apparecchiature di rete, siano esse parte del cablaggio o wireless, inclusi i dispositivi operanti come firewall, utilizzati dall'Amministrazione, nonché di monitorare l'infrastruttura della rete geografica dell'Amministrazione (WAN) attraverso l'utilizzo degli strumenti messi a disposizione dal fornitore assegnatario dei servizi di connettività in rete geografica.

Tale servizio dovrà essere realizzato con adeguato personale tecnico, che garantisca il corretto e completo funzionamento di tutti gli aspetti di configurazione dei vari apparati costituenti il sistema e l'integrazione con tutti i sistemi appartenenti alla infrastruttura di rete.

La Ditta avrà anche il compito di supportare il personale tecnico dell'Amministrazione, per le problematiche di rete e nella fase di troubleshooting.

Il Fornitore deve garantire la continuità di esercizio delle reti anche a fronte di problemi particolarmente complessi.

In particolare, il servizio:

- gestisce l'indirizzamento IP secondo gli standard concordati con l'Amministrazione, la nomenclatura/indirizzamento dei server e dei posti di lavoro, nonché i parametri di configurazione e di QoS;
- prevede la razionalizzazione dell'infrastruttura di rete attiva e passiva, sulla base di quanto concordato con l'Amministrazione;
- prevede l'implementazione e la gestione dei sistemi di problem determination e di analisi degli output a supporto delle applicazioni che utilizzino l'infrastruttura di rete (es. sniffer, sonde);
- effettua configurazione VPN;
- effettua configurazioni VLAN e link aggregation;
- effettua il monitoraggio costante dei parametri significativi della qualità e delle prestazioni della rete;
- coordina ed assicura gli interventi volti al ripristino delle funzionalità del servizio di rete e/o apparati TLC, mediante l'attivazione, a fronte di malfunzionamenti, dei fornitori della manutenzione contrattualizzati dall'Amministrazione;
- modifica regole di instradamento;
- assicura l'effettuazione degli interventi periodici programmati per garantire il buon funzionamento dei sistemi;
- prevede attività di Site Survey per implementazione di nuovi Access Point e verifica di copertura Wi-Fi;
- effettua l'attivazione logica di nuove prese di rete;
- prevede la collaborazione nelle fasi realizzative dei progetti infrastrutturali e/o applicativi che utilizzano l'infrastruttura di rete;
- fornisce un sistema di rendicontazione dei livelli di servizio.

Il servizio comprende anche modifiche di configurazione da apportare agli apparati di rete in quantità massiva, secondo interventi preventivamente concordati.

4.1.4 Servizi di Sviluppo e Integrazione Architetture e Sistemi

Per **Servizi di Sviluppo e Integrazione Architetture e Sistemi** si intende il complesso delle attività operative necessarie alla messa in produzione di nuovi apparati, sistemi e/o ambienti elaborativi e alla loro integrazione nell'Infrastruttura ICT ovvero ad apportare cambiamenti dell'Infrastruttura non riconducibili ad attività di ordinaria gestione e manutenzione. In particolare, il servizio è deputato alle operazioni di improvement dell'architettura dei sistemi, alle attività di assessment, alla migrazione di apparati obsoleti, consolidamento di architetture, virtualizzazione di apparati fisici (e operazioni inverse).

L'infrastruttura può comprendere server distribuiti, il software di base, middleware, DBMS, application server, gli apparati di rete, i dispositivi di storage e backup e comunque tutte le apparecchiature necessarie al corretto funzionamento dei servizi ovunque disposte nell'infrastruttura di proprietà dell'Amministrazione negli stabili di sua proprietà o di terzi ovvero noleggiata da terzi anche in cloud.

Finalità del servizio è la realizzazione, ovvero installazione, test ed avviamento dell'infrastruttura tecnologica, sulla base di Specifiche Tecniche e/o Funzionali prodotte e/o approvate dall'Amministrazione.

Tra le varie attività da eseguire sono compresi:

- il disegno dei sistemi ed il loro dimensionamento;
- l'installazione e l'interconnessione degli apparati di rete, l'integrazione tra i diversi componenti dell'infrastruttura, con contestuale configurazione;
- l'installazione e la configurazione dei sistemi, del firmware, del software di base e del middleware e l'integrazione tra i diversi componenti della fornitura;
- la migrazione di prodotti SW già presenti nel contesto tecnologico dell'Amministrazione ovvero l'aggiornamento alle versioni di recente rilascio di prodotti di mercato;
- la migrazione dei Sistemi Operativi, del middleware, dei server e dei client, per il mantenimento delle versioni ufficialmente supportate e per l'adeguamento dei sistemi alle esigenze di integrazione ed alle compatibilità applicative;
- la dismissione dei vecchi apparati comprensiva delle attività legate alla rottamazione (trasporto compreso) e cancellazione/distruzione dei dati.
- fornire un supporto progettuale e tecnologico centralizzato a tutte le strutture, le piattaforme applicative e tecnologiche dell'Amministrazione;
- incrementare la qualità di erogazione dei servizi forniti dai sistemi dipartimentali tramite la progettazione, l'implementazione e il collaudo di nuove procedure e nuove infrastrutture

tecnologiche;

- progettare, implementare e collaudare nuove soluzioni in ambito infrastruttura, software di base e middleware applicativo, per piattaforme di sviluppo, test e produzione;
- redigere e aggiornare la documentazione specialistica connessa alle attività oggetto della fornitura (sia per attività tecniche di supporto specialistico sia per attività progettuali e di nuova implementazione);
- affiancare e addestrare il Team dedicato alla Conduzione Operativa alla presa in carico delle nuove soluzioni ed architetture implementate per l'Amministrazione;
- predisporre e manutenere i piani di test per tutti i processi di migrazione di servizi su nuove architetture.

Fanno inoltre parte dell'evoluzione dei sistemi le seguenti attività:

- il supporto al capacity management delle infrastrutture informatiche;
- il supporto alla definizione di piani di disponibilità e continuità operativa delle infrastrutture;
- il supporto alla definizione dei processi di service management;
- il supporto alla gestione sistemi per attività che richiedano competenze specifiche;
- il supporto specialistico per gli aspetti tecnologici relativi allo sviluppo applicativo.
- progettare, implementare e collaudare l'evoluzione dell'infrastruttura SAN (predisposizione del piano di deploy della nuova architettura, del piano migrazione e di test, ecc.);
- progettare, implementare e collaudare l'evoluzione delle soluzioni inerenti l'ambiente di posta;
- progettare, implementare e collaudare l'evoluzione dei sistemi di monitoraggio e dei sistemi di reportistica e di datawarehouse per offrire indicatori quantitativi e qualitativi sull'erogazione dei servizi IT;
- progettare, implementare e collaudare l'evoluzione degli application server;
- progettare, implementare e collaudare l'evoluzione dei database server e sistemi software enterprise (ERP, datawarehousing, ecc.);
- progettare, implementare e collaudare l'evoluzione dei sistemi di bilanciamento e dei reverse proxy;
- progettare, implementare e collaudare l'evoluzione dei sistemi di backup/restore dei servizi IT;
- progettare, implementare e collaudare i sistemi e i piani di Business continuity e/o disaster recovery ove richiesto.

Fanno inoltre parte dello sviluppo sistemi le seguenti attività:

- analisi dell'impatto implementativo;
- analisi del rischio;
- analisi dei costi e dei benefici;
- definizione delle modalità di realizzazione;
- definizione dei metodi di collaudo;
- definizione dei metodi di installazione;
- documentazione funzionale;
- procedure operative;
- rilascio della soluzione implementata alla gestione (esercizio).

Al Fornitore può essere richiesta la predisposizione di ambienti prototipali da rendere disponibili per "proof of concept" (POC) o piccole sperimentazioni, con cui verificare le caratteristiche principali della soluzione prima del suo inserimento nell'ambiente operativo, sull'Infrastruttura dell'Amministrazione. Dopo la verifica delle funzionalità del prototipo si eseguono le installazioni nell'ambiente di destinazione finale.

Tutte le attività sopra descritte prevedono l'aggiornamento e/o la predisposizione della documentazione a supporto (dettaglio dell'installazione, delle configurazioni e delle procedure di gestione, di salvataggio della configurazione, script di start/stop dei prodotti, dipendenze con altri server ecc.).

4.1.5 Servizi di Rete: progettazione e sviluppo

I "Servizi di Rete, Progettazione e Sviluppo" sono servizi deputati alle operazioni di improvement dell'architettura di rete, nonché delle attività di verifica ed eliminazione delle obsolescenze eventualmente in essere.

In particolare, il servizio in oggetto:

- Effettua la migrazione degli apparati obsoleti verso nuove architetture, previa collaborazione nell'analisi con i servizi di cybersecurity;
- Si occupa della sostituzione di apparati riportando puntualmente la configurazione esistente sugli apparati di nuova immissione garantendo, quindi, la continuità del servizio;
- Effettua la progettazione di nuove sezioni/sottoreti;
- Effettua la verifica dei carichi di rete eventualmente procedendo alla rimodulazione degli stessi mediante suddivisioni e/o applicando politiche di QoS;
- Provvede all'efficientamento dei percorsi di routing allo scopo di ridurre i tempi di latenza incrementando quindi la velocità di scambio dati ovvero progetta "rotte" alternative al fine di poter garantire la continuità operativa sebbene attraverso instradamenti meno efficienti;

- Supporta l'identificazione delle possibilità di comunicazioni non cablata (wireless) quali punto-punto, WLAN, satellite, identificando le diverse caratteristiche e l'applicabilità a diverse necessità aziendali di trasmissione;
- Progetta collegamenti non cablati punto-punto, in termini di pianificazione geografica, calcolo di perdita del percorso, verifica delle ellissi di Fresnel e predisponendo i test da effettuare per valutare il percorso;
- Supporta l'identificazione di collegamenti basati su satellite, verificando diversi parametri e pianificando il tipo di trasferimento dati che può utilizzare tali collegamenti sia di norma sia come soluzione di ripiego;
- Pianifica, supervisiona la realizzazione ed effettua i test dei collegamenti digitali a infrarossi tra reti diverse;
- Supporta la pianificazione di diverse implementazioni della 'convergenza digitale', dal "data streaming" (sia voce che video), al VoIP (non solo a due vie ma anche conferenze audio-video), proponendo architetture, protocolli e schemi differenti;
- Supporta la pianificazione, supervisiona la realizzazione ed effettua i test di accettazione dei sistemi digitali di trasmissione, sotto forma di nuova "Radio digitale" e "TV digitale" (DRM, DAB);
- Raccoglie dati campione e li utilizza per costruire un modello pilota significativo del nuovo sistema. Rende più solido il modello generale tramite diverse sessioni di simulazione in cui i responsabili aziendali, i responsabili di processo e gli utenti operativi del sistema informativo possono comprendere e approvare pienamente le modalità di esercizio del sistema finale addivenendo quindi ad una progettazione esecutiva;
- Produce documenti e rapporti scritti di alta qualità, in cui vengono descritti argomenti organizzativi e/o tecnici con uno stile chiaro e conciso;
- Collabora con il personale IT dell'Amministrazione sia per il collaudo (nuovo modulo singolo o intero sistema) che per l'estrazione, la trasformazione e il caricamento dei dati;
- Conduce le simulazioni finali con dati reali e i test di accettazione, anche per conto dell'Amministrazione se supportato da opportuna delega;
- In conformità agli accordi presi supporta l'azienda cliente durante la fase iniziale di utilizzo del nuovo sistema e nella misurazione dei suoi vantaggi attraverso eventuali revisioni post-implementazione;

4.1.6 Servizi di Service e Performance Management

È compito del Fornitore assicurare che i servizi di gestione IT siano organizzati e strutturati secondo un approccio process-driven, in cui la complessa struttura organizzativa/operativa dei servizi sia scomposta in una serie di processi integrati e correlati tra loro in accordo con le best practices ITIL, con l'obiettivo di:

- migliorare la qualità dei servizi IT;
- ridurre i costi di erogazione dei servizi;
- allineare i servizi IT con i bisogni correnti e futuri del business e dei clienti.

Nel caso in cui l'Amministrazione abbia già definito a priori la strutturazione dei processi di gestione secondo le best practices ITIL, il Fornitore dovrà erogare i servizi adottando i processi già definiti; nel caso in cui, invece, l'Amministrazione non abbia definito, in tutto o in parte, la strutturazione dei processi di gestione, il Fornitore dovrà, su richiesta e in accordo con l'Amministrazione, proporre e adottare un'adeguata strutturazione dei processi previsti.

Si ritiene utile sottolineare, in maniera più puntuale, il valore aggiunto atteso dall'operatività del Fornitore nell'ambito di alcuni tra i processi più significativi per l'evoluzione del modello di erogazione dei servizi.

Si precisa che non tutti i processi per cui ci si attende un impegno dal Fornitore sono di seguito elencati, fermo restando che il Fornitore deve supportare l'Amministrazione effettuando tutte le attività di competenza, sulla base di quanto stabilito nelle procedure operative che saranno rese disponibili o implementate nel corso della gestione contrattuale.

4.1.6.1 Gestione delle Richieste e delle Segnalazioni

In coerenza con i processi in uso presso l'Amministrazione, è richiesto che il Fornitore utilizzi gli strumenti resi disponibili dall'Amministrazione per tracciare le attività a carattere operativo nonché le richieste di informazioni e di segnalazione di disservizio.

In particolare, il Fornitore stesso deve:

- alimentare gli strumenti di tracciatura;
- effettuare la ricezione e la presa in carico delle richieste nei tempi concordati;
- aggiornare le informazioni di ciascun ticket con l'effettivo stato/andamento delle attività;
- fornire una stima dei tempi di esecuzione e una diagnosi relativa all'intervento da effettuare;
- effettuare la chiusura dei ticket;
- gestire, per quanto di competenza, gli interventi dei fornitori terzi.

4.1.6.2 Supporto al Processo di Incident e Problem Management

Al fine di garantire la corretta fruizione dei servizi da parte dell'utenza di riferimento, il Fornitore è responsabile della gestione di tutti i casi in cui sia rilevabile una interruzione o un degrado nella fruizione del servizio. Tale responsabilità è indipendente dalla causa dell'interruzione/degrado, che può essere legato al software, all'hardware e relativo firmware sistemi e/o apparati di rete.

Il Fornitore è tenuto ad effettuare le attività necessarie al ripristino del servizio all'utenza di riferimento entro i tempi massimi prefissati, anche attraverso l'attivazione delle procedure di escalation concordate.

Tali procedure tengono conto del livello di gravità del malfunzionamento e dell'impatto dello stesso sull'operatività dell'utenza.

L'attività di gestione dei malfunzionamenti deve essere sia proattiva, ossia rivolta alla prevenzione, sia reattiva, ossia rivolta alla gestione ed infine alla risoluzione di tutti gli eventi che comportano l'interruzione o il degrado nella fruizione del servizio.

Pertanto, tra le attività richieste si includono:

- l'identificazione del malfunzionamento, la sua documentazione, la gestione delle comunicazioni e dell'escalation e la sua risoluzione, anche attraverso l'attività di terze parti;
- l'analisi del verificarsi di problemi ripetitivi. I risultati dell'analisi sono inseriti nella knowledge base e sugli elementi interessati sono eseguiti controlli approfonditi atti ad individuare e risolvere problemi di tipo strutturale, secondo quanto concordato con la l'Amministrazione nell'ambito del processo di Problem management;
- l'analisi delle informazioni derivanti dall'esecuzione delle attività di verifica di performance dei sistemi, tenendo conto delle informazioni provenienti dai sistemi di monitoraggio.

In ultimo, è responsabilità del Fornitore il salvataggio dei dati ai fini dell'analisi di incidenti di sicurezza. Il Fornitore deve assicurarsi che i sistemi, anche non direttamente gestiti, inviino al sistema di Log Management le informazioni utili alle attività di analisi, attivando - in caso negativo - le procedure concordate con l'Amministrazione.

È richiesto, infatti, che sia effettuata la conservazione di tutti i log di auditing relativi a web server, application server, apparati di sicurezza e quanto altro possa essere necessario alla ricostruzione di comportamenti insidiosi e per l'individuazione di possibili responsabilità penali e civili conseguenti a condotte illecite. Tali log devono essere mantenuti in linea per il periodo concordato con l'Amministrazione. Su tali log l'Amministrazione si riserva di richiedere al team di effettuare ricerche ed elaborazioni statistiche puntuali.

Si precisa che i dati da raccogliere e da salvare ai fini dell'indagine sugli incidenti di sicurezza saranno concordati successivamente all'avvio della fornitura.

4.1.6.3 Supporto al Processo di Change e Release & Deployment Management

Al fine di garantire il corretto funzionamento, lo sviluppo e l'evoluzione dell'infrastruttura ICT dell'Amministrazione, il Fornitore è responsabile della pianificazione, dell'attuazione, del tracciamento e della verifica dei cambiamenti dell'hardware, del firmware, dell'evoluzione dei sistemi operativi, dei prodotti programma/middleware, dei prodotti applicativi e delle relative correzioni coerentemente con i processi di Change Management e Release & Deployment Management.

4.1.6.4 Supporto al Processo di Service Asset & Configuration Management

Il Fornitore deve garantire il costante, accurato e continuo allineamento delle basi dati del CMDB; nel caso in cui tali aggiornamenti non possano essere eseguiti automaticamente, il Fornitore deve procedere con l'aggiornamento manuale. Si precisa che l'aggiornamento del CMDB è prevalentemente effettuato in automatico attraverso prodotti di scansione le cui politiche sono definite dall'Amministrazione e sono supportati da script/procedure automatiche che potrebbero essere realizzate da terzi.

Si precisa che i processi e le procedure operative sono oggetto di revisione e miglioramento continuo, pertanto, nel periodo contrattuale, le modalità indicate potrebbero variare. In ogni caso i fornitori sono obbligati a seguire qualsiasi variazione dei processi e delle procedure operative che l'Amministrazione indicherà.

L'aggiornamento costante e accurato della baseline, in particolare del CMDB, è ritenuto il nucleo fondamentale sui cui si fondano:

- i processi già in uso nonché i processi che potrebbero essere eventualmente adottati ed implementati nel corso della durata contrattuale;
- il patrimonio informativo relativo alla consistenza e alla configurazione dell'infrastruttura ICT dell'Amministrazione;
- la valutazione di eventuali impatti per i servizi di business dell'Amministrazione a fronte di evoluzioni, cambiamenti di carattere infrastrutturale;
- le analisi volte all'integrazione e/o all'introduzione di nuovi servizi a supporto dell'attività istituzionale dell'Amministrazione;
- la rilevazione e la misurazione della qualità del servizio all'utenza di riferimento.

Si ritiene utile precisare che, alla data di inizio attività, il CMDB potrebbe non essere completo di tutte le informazioni previste sia in termini di CI che di attributi previsti.
Ad inizio fornitura, è richiesto al Fornitore un assessment sulla consistenza e coerenza dei dati di Asset & Configuration e delle relazioni tra gli stessi.

4.1.6.5 Supporto al Processo Capacity Management

Il Fornitore è responsabile dell'esecuzione delle attività operative a supporto del processo di Capacity Management. Pertanto, è responsabile della raccolta dei dati, dell'analisi periodica dello stato di salute dell'Infrastruttura ICT affidata in gestione, dell'analisi dei trend di carico e della produzione di reportistica che mostri la situazione riassuntiva di ciascun sistema e che ne evidenzi eventuali criticità o necessità di evoluzione.
Si precisa che l'Amministrazione si riserva di richiedere la produzione di ulteriore reportistica il cui contenuto, formato e periodicità è concordato ad inizio fornitura ed eventualmente rivisto, nel corso della durata dei servizi, ai fini della predisposizione del Piano della Capacità.
Il Fornitore, nell'erogazione del servizio, può utilizzare gli strumenti e i prodotti resi disponibili dall'Amministrazione ovvero può utilizzare script e/o le funzionalità native del software di sistema.

4.1.6.6 ServiceDesk Sistemistico

Nell'ambito dei processi strutturati di Service Management, il Fornitore deve prevedere (se richiesto dall'Amministrazione) una funzione di Service Desk Sistemistico, che agisca come punto di contatto tra i referenti informatici dell'Amministrazione e l'IT Service Management, per gestire incidenti e richieste degli utenti e fornire un'interfaccia per gli altri processi, quali Change, Problem, Configuration, Release, ecc., gestendo tutto il ciclo di vita dell'incidente o della service request.
Gli elementi distintivi della funzione di Service Desk Sistemistico sono:

- prima diagnosi e tentativo di risoluzione delle segnalazioni/richieste al primo livello, anche attraverso l'utilizzo delle informazioni presenti nella Knowledge base;
- classificazione degli incidenti o richieste, attraverso modalità obiettive per classificare gli incidenti in modo che siano assegnati opportunamente;
- assegnazione della priorità, attraverso modalità obiettive per l'assegnamento della priorità di un incidente (ad esempio attraverso una matrice di impatto/urgenza);
- assegnazione degli incidenti/richieste, automatizzando il più possibile il routing dei casi in base al workload e alle competenze di ogni tecnico, in modo da ottimizzare le risorse;
- assegnazione a gruppi esterni, attraverso accordi con Fornitori terzi responsabili di specifiche attività.

La funzione di service desk sistemistico è relativa alle problematiche di system management descritte nel presente Capitolato Tecnico e ha come principale utenza di riferimento i referenti informatici dell'Amministrazione. Non è compresa l'assistenza agli utenti per problematiche che esulano dal contesto suddetto, quali ad esempio supporto alla gestione delle postazioni di lavoro o supporto all'utilizzo delle funzioni applicative.

4.2 Lotto 2 – Sicurezza Informatica

Il Lotto 2 annovera al suo interno un insieme di servizi e attività inerenti alla sicurezza informatica, inclusi i servizi di monitoraggio in tempo reale di eventi di sicurezza, la progettazione e lo sviluppo di soluzioni atte a garantire il livello adeguato di sicurezza rispetto al contesto IT aziendale, incluso il governo degli aspetti di sicurezza informatica nel loro complesso. Considerata la complessità e soprattutto la criticità dei servizi e delle attività ricomprese nel presente Lotto, in stretta sinergia con quelle di ambito più prettamente sistemistico e infrastrutturale, è necessario e fondamentale precisare che deve essere garantita la massima disponibilità al fine di una piena e stretta collaborazione con le figure professionali dell'IT, interno all'Ente, del Fornitore dei servizi di System Management o di eventuali altre figure professionali che operano per conto dell'Amministrazione.
Di seguito l'elenco dei Servizi inerenti il presente Lotto.

4.2.1 Servizio di Monitoraggio in tempo reale di eventi di sicurezza (SOC)

Il **"Servizio di Monitoraggio in tempo reale di eventi di sicurezza**" comprende tutte le attività di monitoraggio dell'infrastruttura IT dell'Amministrazione al fine di rilevare e gestire in tempo reale gli eventi relativi alla sicurezza informatica. Il servizio è erogato dal **SOC – Security Operation Center.**

In particolare, il SOC effettua il monitoraggio degli eventi dell'insieme delle risorse IT dell'organizzazione: server, endpoint, reti ed apparati di rete, software di sistema, applicazioni, utenze, ecc… al fine di rilevare falle di sicurezza, tentativi di intrusione o di attacco ed ogni altra tipologia di attività sospetta, quale a puro titolo esemplificativo e non esaustivo: attività compiuta da malware, sfruttamento di vulnerabilità anche di tipo Zero-Day, Targeted and Advanced Persistent Threat (APT), Privilege Escalation, movimenti laterali, attacchi ad applicazioni, frodi informatiche, Denial of Service (DDos, DoS), ecc…

Pertanto, il Fornitore deve disporre del servizio SOC all'interno del proprio Centro Servizi per l'Operatività da Remoto, da mettere a disposizione delle Amministrazioni che facciano richiesta di servizi da erogare mediante tale modalità operativa.

La lingua di riferimento per l'erogazione dei servizi deve essere l'italiano.

Da tale Centro, attraverso l'utilizzo degli opportuni strumenti e mediante l'impiego di personale specializzato, il Fornitore dovrà avere la possibilità di operare in collegamento con i sistemi dell'Amministrazione per effettuare tutte le attività previste dal servizio, ad esempio:

- controllare costantemente (sulla base delle finestre di erogazione del Servizio concordate con l'Amministrazione) il sistema di monitoraggio per poter intervenire immediatamente in caso di attivazione di allarmi;

- investigare e definire la natura delle anomalie rilevate e attribuirle ad eventuali minacce e problemi di sicurezza;
- svolgere un primo livello tecnico in ambito sicurezza rilevando, investigando e assegnando priorità alle minacce, identificando gli eventuali sistemi ed utenti impattati, mettendo in atto azioni ed attività al fine di mitigare o annullare l'impatto di minacce o incidenti;
- ricevere, qualificare e gestire richieste di assistenza che potranno generarsi dal sistema di monitoraggio o tramite chiamata sia di personale dell'Amministrazione, sia di Help-desk di società terze che forniscono servizi di manutenzione su sistemi hardware e software utilizzati dall'Amministrazione stessa;
- collaborare in sinergia con il NOC ed il personale IT dell'Amministrazione;
- contattare ed informare costantemente il personale dell'Amministrazione qualora ve ne sia la necessità (sulla base di procedure concordate con l'Amministrazione);
- gestire in autonomia gli allarmi, contattando eventualmente il personale di fornitori terzi (sulla base di procedure concordate con l'Amministrazione);
- effettuare gestione, verifica, analisi, correlazione, storicizzazione e conservazione a norma delle informazioni raccolte nei file di log delle infrastrutture di sicurezza e di rete e degli allarmi generati;
- essere un single point of contact attivo e raggiungibile (sulla base delle finestre di erogazione del Servizio concordate con l'Amministrazione) tramite numero di telefono ed e-mail;
- provvedere ad inviare periodicamente (con cadenza concordata con il personale dell'Amministrazione), tramite comunicazione e-mail, un riepilogo degli allarmi attivati e risolti e di eventuali criticità in atto;
- generare Report di Sicurezza con i dati collegati alle attività di gestione della sicurezza; periodicità e tipologia dei report generati verranno concordati con l'Amministrazione.
-

Tutto il personale del SOC deve essere in grado di prendere in carico tutte le attività relative all'infrastruttura dell'Amministrazione, al fine di garantire una continuità di servizio al Committente; a tal fine, pertanto, il Fornitore deve adeguatamente formare ed istruire il personale del SOC relativamente all'infrastruttura ICT dell'Amministrazione stessa.

Il SOC del Fornitore deve rispettare inoltre le seguenti regole:

- la connessione telematica tra il Centro Servizi e le sedi dell'Amministrazione deve essere realizzata attraverso canale dedicato punto-punto a costo del Fornitore. Nessun onere potrà essere ascritto all'Amministrazione. Si intende ricompresa nella

connessione anche la dotazione degli apparati di networking ed ogni altra dotazione necessaria, inclusi i cablaggi dalla terminazione di rete del Provider del collegamento ai locali CED dell'Amministrazione qualora se ne presentasse la necessità. La soluzione deve garantire adeguate prestazioni e affidabilità in caso di malfunzionamento di uno dei componenti dell'infrastruttura;

- il Fornitore deve predisporre presso il proprio Centro Servizi una soluzione tecnologica avente prestazioni e affidabilità adeguate anche in caso di malfunzionamento di uno dei componenti dell'infrastruttura, tale in sostanza a garantire connettività ed operatività ai gruppi impegnati nell'erogazione dei servizi.

  In particolare:

  a) **Un punto di accesso alla rete dell'Amministrazione**. In particolare, il Fornitore dovrà garantire che gli accessi alla rete ed ai sistemi dell'Amministrazione avvengano esclusivamente dal personale identificato mediante **utenze nominative** autorizzate dal proprio sistema di gestione degli accessi. Per quanto riguarda l'accesso ai sistemi di proprietà dell'Amministrazione, il Fornitore dovrà utilizzare utenze nominative nelle modalità concordate con l'Amministrazione, compatibilmente alle specifiche tecnologie e sempre in conformità con quanto previsto dal provvedimento del Garante in materia di accesso degli amministratori di sistema. Non è richiesta la realizzazione di un sistema di Single Sign On che consenta l'uso delle medesime credenziali nei due domini (Sistemi del Centro servizi e Sistemi dell'Amministrazione);

  b) **Autenticazione e profilazione delle utenze.** Il processo di autenticazione e profilazione dell'utente è riferito al punto di accesso alla rete dell'Amministrazione;

  c) **Tracciatura degli accessi ai sistemi**. In ottemperanza al provvedimento del Garante per la protezione dei dati personali, in materia di accessi degli amministratori di sistema, dovrà essere possibile registrare gli accessi e le attività eseguite dal personale del SOC sul sistema per la gestione degli accessi del Centro Servizi, ad es. login, ssh, desktop remoto. Per quanto riguarda la registrazione degli accessi e delle attività degli Amministratori su ciascun sistema di proprietà dell'Amministrazione, le modalità saranno concordate con l'Amministrazione stessa;

d) **Conservazione dei Log**. È richiesta la conservazione per almeno un anno dei log del sistema di gestione degli accessi, utilizzato per l'accesso alla rete ed ai sistemi dell'Amministrazione. Lo strumento di conservazione e di gestione dei log deve essere predisposto dal Centro servizi del Fornitore, senza alcun onere per l'Amministrazione, che si riserva di richiedere tali log con frequenza periodica in base alle procedure concordate con il Fornitore stesso.

- il Fornitore deve garantire la sicurezza del collegamento e la riservatezza dei sistemi e delle informazioni attraverso la formalizzazione e l'applicazione di procedure e politiche di sicurezza da adottare al proprio interno, adeguate ai requisiti stabiliti. Infatti, è responsabilità del Fornitore assicurare che il Centro Servizi, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni da e verso la rete dell'Amministrazione siano protette mediante l'adozione di adeguati sistemi e metodologie definite utilizzando come riferimento le norme della serie ISO/IEC 27001. In particolare, nell'esecuzione dei servizi, il Fornitore deve garantire l'evoluzione, la manutenzione e l'adeguamento tecnologico dei sistemi, delle reti e di tutti gli strumenti impiegati presso il Centro Servizi che si rendano necessarie a soddisfare i requisiti di sicurezza stabiliti, nonché l'aggiornamento delle politiche di sicurezza e delle contromisure attuate e la risoluzione reattiva o proattiva di incidenti di sicurezza.

In considerazione dell'esigenza di garantire il massimo grado di copertura di tutti gli aspetti di sicurezza, si richiede la redazione di un Piano della Sicurezza in conformità a best practice e/o a standard internazionali, secondo quanto concordato con l'Amministrazione.

Nella tabella seguente si riportano alcuni requisiti da intendersi come minimi e imprescindibili:

Categoria	Requisiti Minimi
Sicurezza delle reti	Il punto di accesso alla rete dell'Amministrazione deve essere adeguatamente protetto mediante sistemi firewall che operino secondo modalità note come "Stateful Inspection". Devono essere utilizzati sistemi/meccanismi di "Intrusion Detection and Prevention" che analizzino il traffico in entrata ed in uscita dalla rete dell'Amministrazione.
Riservatezza dei dati e delle trasmissioni	Deve essere garantita la riservatezza di tutti i dati gestiti.

Categoria	Requisiti Minimi
Integrità dei dati	Devono essere adottati antivirus centralizzati ad aggiornamento periodico, che analizzino e bonifichino gli eventuali codici malevoli. Devono essere adottati antivirus su tutte le postazioni utilizzate dal personale del Fornitore e collegate con la rete dell'Amministrazione. Tali postazioni devono soddisfare lo standard per le postazioni di lavoro previste per l'Amministrazione
Auditing e vulnerability assessment	Devono essere registrati tutti gli eventi telematici che hanno impatto sui sistemi, effettuati dal Centro servizi del Fornitore, permettendo la ricostruzione di comportamenti insidiosi e/o malevoli e l'individuazione di possibili responsabilità penali e civili conseguenti condotte illecite. Tali registrazioni dovranno essere effettuate e conservate sui sistemi del centro servizi che consentiranno l'accesso alla rete dell'Amministrazione, ovvero sui sistemi dell'Amministrazione, secondo le modalità concordate con l'Amministrazione.
Amministrazione accessi	Devono essere adottati adeguati processi di Amministrazione degli accessi (fisici e logici) effettuati nel Centro servizi che prevedano l'identificazione delle diverse categorie di utenti, la definizione dei corrispondenti profili di autorizzazione e delle modalità di rilascio dell'accesso.

Il Fornitore deve adottare una soluzione tecnico-organizzativa atta a garantire la continuità dell'erogazione dei servizi anche in caso di evento disastroso e/o di interruzione della connessione tra il Centro Servizi e la rete dell'Amministrazione, e il rispetto dei requisiti di qualità contrattuali.

Il Fornitore deve erogare il servizio secondo una delle due seguenti modalità, a discrezione dall'Amministrazione sulla base delle proprie caratteristiche e risorse:

- mettendo a disposizione una propria piattaforma di monitoraggio degli eventi di sicurezza dotata di appositi moduli di detection, agenti o dispositivi da installare presso i sistemi dell'Amministrazione, in grado di raccogliere le informazioni atte ad individuare gli scenari di rischio ed attacco come sopra indicati;
- utilizzando le piattaforme già eventualmente in utilizzo presso l'Amministrazione committente comprese quelle di asset management, CMDB, e di ticketing per tracciare le attività a carattere operativo nonché le richieste di informazioni e di segnalazione di incidente.

Nella prima modalità, il Fornitore dovrà mettere a disposizione una piattaforma web che permetta all'Amministrazione di accedere ad apposite dashboard configurate opportunamente per consentire la consultazione delle anomalie rilevate, degli allarmi attivati e lo storico degli stessi, l'accesso a tutte

le informazioni inerenti le diverse fasi di gestione degli incidenti ed alle informazioni generate dai moduli di detection.

Gli eventi generati dalla piattaforma di monitoraggio e dai moduli di detection dovranno essere collezionati in appositi log e messi a disposizione dell'Amministrazione, su richiesta.

La raccolta e la cifratura dei log effettuata dalla piattaforma di monitoraggio deve garantire la catena di custodia, l'apposizione dei time stamp di ricezione da parte di ogni componente, il formato non modificabile del log con o senza la conservazione del raw event, l'hashing effettuato nel database per impedire la cancellazione selettiva dei log, la presenza di audit log di accesso alla piattaforma, nonché la compressione e la cifratura degli archivi.

All'attivazione del contratto saranno definiti e formalizzati i processi da applicare alla gestione degli allarmi e degli incidenti di sicurezza con specifico riferimento agli aspetti di comunicazione, responsabilità ed escalation tra il Fornitore, l'Amministrazione ed eventuali altri terzi coinvolti nella reazione e gestione (es. fornitori applicativi).

Sarà altresì compito del servizio **SOC** la rilevazione dei livelli di sicurezza (antivirus e allineamento delle configurazioni alle policy di sicurezza dei sistemi dell'Amministrazione). Il servizio è anche deputato all'analisi e verifica dei livelli di sicurezza complessiva dell'architettura e della valutazione di eventuali azioni di perfezionamento della security stessa.

Può essere coinvolto fattivamente anche nella progettazione di contromisure ad attacchi e tentativi di intrusione, inserimento e progettazione di nuove e più efficaci regole di protezione nonché l'esecuzione di test e simulazioni di attacco ed intrusione (VA/PT), necessari anche a valutare le corrette configurazioni e correlazioni oltre ai tempi di risposta.

In particolare, il servizio in oggetto ha in carico le seguenti attività:

- collabora col personale dell'Amministrazione e del NOC per fornire informazioni di dettaglio su aspetti di sicurezza per apparati di rete e sistemi obsoleti e per le nuove architetture (patching, hardening, protocolli da disattivare, etc);
- verifica i connettori per la raccolta dei log e delle correlazioni per generare allarmi, controllando il corretto funzionamento e le corrette informazioni a fronte dell'introduzione di nuovi servizi e architetture;
- effettua le attività di assessment degli apparati di monitoraggio per garantire che la raccolta delle informazioni sia sempre attiva ed efficace a garanzia di allarmi in real-time.

4.2.2 Servizio di Conduzione Operativa di Apparati e Sistemi di Sicurezza

È richiesto al Fornitore di erogare servizi di sicurezza in una modalità atta a gestire apparati di sicurezza informatica in produzione presso l'Amministrazione.

In particolare, i servizi previsti, a titolo esemplificativo e non esaustivo, sono:

- Servizio di gestione dei dispositivi di sicurezza perimetrale: il servizio consente di attuare la politica per la sicurezza sui dispositivi di difesa perimetrale dell'Amministrazione (per es. Firewall, VPN);
- Servizi di Next Generation firewall;
- Servizi di Web Application firewall;
- Servizio di Content Filtering. Il servizio permette di ottimizzare l'uso delle risorse infrastrutturali, quali la capacità di banda verso Internet od il sistema di posta elettronica, controllando l'ammissibilità dei contenuti in transito rispetto alle politiche di sicurezza definite;
- Servizio di Content Security (antivirus, antimalware, anti-ransomware). Il servizio provvede ad una gestione efficace delle contromisure atte a contrastare la diffusione dei codici malevoli, quali virus o worm su sistemi sia client (postazione di lavoro) che server;
- Servizio IDS (Intrusion Detection System) / IPS (Intrusion Prevention System): il servizio fornisce la valutazione di eventi, situazioni anomale od allarmi che possono rappresentare una minaccia per la sicurezza dell'infrastruttura attraverso opportuni strumenti di rilevazione;
- Servizio SIEM: il servizio fornisce un raggruppamento di vari sistemi di sicurezza (log collection, analisi dei log, correlazione di eventi, funzionalità di alerting e di archivio) in un ambiente unitario al fine di valutare le minacce e di gestire i rischi di sicurezza;
- Servizio SOAR - Security Orchestration, Automation, and Response: il servizio fornisce un insieme di soluzioni software che permettono di gestire in modo coordinato i processi di gestione delle vulnerabilità, di risposta agli incidenti e di automazione delle attività di sicurezza;
- Servizio di telemetria, xDR/EDR/NDR: server, mail, endpoint, reti detection and response;
- Servizio di Threat Sharing per la gestione degli Indici di Compromissione (IoC) e per la condivisione degli stessi con il Fornitore e con altre Organizzazioni; all'integrazione con i sistemi di sicurezza dell'amministrazione.

Per **"Conduzione Operativa Apparati e Sistemi di Sicurezza"** si intende il complesso delle attività riconducibili all'ordinaria gestione e manutenzione dell'infrastruttura di sicurezza informatica garantendone il funzionamento e l'efficienza, la copia e backup delle configurazioni degli apparati in aderenza a quanto previsto dall'apposito piano, qualora esistente. Il Fornitore deve garantire la continuità di esercizio degli apparati e sistemi di sicurezza anche a fronte di problemi particolarmente complessi.

Gli obiettivi della conduzione operativa sono:

- garantire la disponibilità dei sistemi e l'esecuzione delle attività schedulate;
- assicurare un continuo controllo sullo stato dei sistemi e dei collegamenti, individuare criticità o malfunzionamenti ed intraprendere le azioni necessarie;
- garantire l'efficienza dei sistemi rispetto all'utilizzo delle risorse hardware e software;
- controllare l'impatto sulla tecnologia esistente e garantire l'adeguamento degli ambienti elaborativi a fronte dell'immissione in esercizio di modifiche correttive e/o evolutive di applicazioni e sistemi esistenti;
- monitorare e verificare i consumi effettivi degli eventuali servizi in cloud.

4.2.3 Servizio di Vulnerability Assessment

È richiesto al Fornitore la pianificazione e l'esecuzione dei test di vulnerabilità concordati con l'Amministrazione e da essa supervisionati. I test verranno effettuati con cadenza periodica al fine di verificare il livello di efficacia delle Politiche di Sicurezza. In tale ambito sarà richiesto al Fornitore di contribuire fattivamente all'implementazione delle eventuali azioni correttive per la rimozione delle criticità individuate, in collaborazione coi tecnici del IT dell'Amministrazione, sia per la parte di controllo e revisione delle politiche di configurazione, sia per interventi specifici di host hardening sui sistemi server e storage.

Nelle variazioni delle Politiche di Sicurezza, i nuovi requisiti o le modifiche dei requisiti esistenti saranno implementati mediante un processo specifico che prevede la progettazione, l'implementazione e messa in esercizio da parte del Fornitore dei cambiamenti alle infrastrutture tecnologiche e/o alle modalità di erogazione dei servizi che si rendessero necessarie.

Il Fornitore si impegna a supportare l'Amministrazione o terzi da essa designati ad implementare le politiche di sicurezza.

4.2.4 Servizio di Vulnerability Management

Il Fornitore deve erogare, per le Amministrazioni che necessitano di un monitoraggio continuo, il servizio di Vulnerability Management le cui modalità di erogazione sono da concordare con le medesime.

Per l'Amministrazione già dotata di un sistema di Vulnerability Management che scansiona sistemi (server, apparati di rete, ecc…), applicazioni, oltre alle infrastrutture containerizzate, si richiede al Fornitore il supporto per la gestione della piattaforma e la predisposizione della reportistica con cadenza periodica sia di alto livello (Executive Summary) che di quella tecnica in cui si evidenzi le eventuali azioni correttive e la rimozione delle criticità da inoltrare alle strutture interne di

competenza, individuate assieme all'amministrazione coinvolta.

Differentemente l'Amministrazione può richiedere al Fornitore la fornitura di una piattaforma "as a service" dotata di appositi moduli di detection, agenti o dispositivi da installare presso i sistemi dell'Amministrazione, con la collaborazione del Fornitore, in grado di raccogliere le informazioni e consentire la produzione dei report nelle stesse modalità sopra riportate.

4.2.5 Attività di Penetration Test

È richiesto al Fornitore di eseguire attività di penetration testing (PT) al fine di rilevare possibili vulnerabilità di tutte le componenti di un sistema informatico dell'Amministrazione e procedere conseguentemente con una pianificazione dei rimedi e relativo innalzamento del livello di sicurezza.

Si riportano alcuni esempi di penetration test, a puro titolo esemplificativo e non esaustivo, che potranno essere richiesti: penetration test esterni, penetration test interni, penetration test mirati, penetration test delle applicazioni web, penetration test VPN, penetration test reti WiFi.

Le modalità dei PT richiesti seguono la classica categorizzazione di black-box, gray-box, white-box in cui al pen-tester viene concessa la minima conoscenza dei sistemi, reti e applicazioni di destinazione fino ad un alto livello di conoscenza che comprende tutta la documentazione che descrive un'applicazione ed il suo ciclo di vita oltre all'accesso con profili diversificati ove presenti.

Per le Amministrazioni in cui sono applicate politiche sullo sviluppo sicuro delle applicazioni, i test dovranno verificare che quanto indicato nella checklist e dichiarato dalla struttura che ha in carico l'applicazione corrisponda a quanto realmente riscontrato.

A fronte di PT negativi sono previsti i relativi re-check.

4.2.6 Servizi di Application Security Testing

Per le applicazioni di un'Amministrazione nell'intero ciclo di vita, SDLC (Software Development Life Cycle), e a garanzia del principio generale di "sicurezza e privacy by design e by default", si rende necessario il test del codice di tipo DAST (Dynamic Application Security Test) e SAST (Static Application Security Test), nonché SCA (Software Composition Analysis) per testare applicativi legacy che utilizzano codici open source o di terze parti.

Tale servizio è generalmente demandato a un fornitore terzo a cui sono state commissionate le applicazioni con il rilascio di specifici report da analizzare e verificare con il supporto dei servizi inclusi in questo capitolato.

Le Amministrazioni potranno richiedere al Fornitore un servizio di analisi del codice sia di applicazioni web-based che mobile, applicazioni Agile e "containerizzate" il cui software (o parte di esso) è di loro proprietà o in riuso, collocate on-premise o in cloud.

4.2.7 Servizi di Incident Response and Remediation

Il Fornitore deve erogare servizi di risposta e remediation degli incidenti di sicurezza.

Questo servizio ha lo scopo di:

- valutare e gestire il rischio associato alle minacce di tipo informatico;
- utilizzare strumenti tecnologici e competenze per affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza.

Il personale deputato al servizio di Incident Response, il secondo livello tecnico in ambito sicurezza informatica, di concerto al team IT (system e/o client), eseguono le necessarie attività per la risoluzione delle anomalie e nell'esecuzione di tutte le azioni necessarie al contenimento degli eventi riferiti dall'incidente nel più breve tempo possibile onde evitare la diffusione su altri sistemi, oltre al supporto e alla verifica per il ripristino degli eventuali servizi compromessi.

Tra le azioni di competenza del Team figurano a puro titolo esemplificativo e non esaustivo:

- identificazione dei sistemi compromessi;
- analisi delle minacce e classificazione del livello di impatto;
- identificazione dei soggetti da coinvolgere ed eventuale apertura di uno specifico ticket o chiamata diretta a soggetti terzi, secondo le modalità concordate con l'organizzazione;
- definire e adottare contromisure al fine di mitigare le conseguenze dell'incidente, neutralizzare le minacce, prevenire ulteriori accessi o danni in modo concordato con l'Amministrazione e coinvolgendo gli altri soggetti deputati alla gestione dell'incidente;
- definire e adottare contromisure di protezione della rete per prevenire ulteriore diffusione di malware in modo concordato con l'Amministrazione e coinvolgendo gli altri soggetti deputati alla gestione dell'incidente;
- isolare i sistemi compromessi (ad esempio da malware) con gli opportuni strumenti e garantire la gestione corretta dell'analisi forense.

Inoltre, dovrà svolgere un'attività di supporto ai processi di gestione dell'incidente da parte dell'Amministrazione, come ad esempio supporto alla redazione dell'incident report e all'enforcement tecnologico in funzione delle informazioni acquisite durante tutte le fasi di gestione dell'incidente.

4.2.8 Servizio di User and entity behavior analytics (UEBA)

Il Fornitore deve erogare il Servizio di User and Entity Behavior Analytics (UEBA), che consiste nell'utilizzo di piattaforme ed algoritmi, nonché di intelligenza artificiale, al fine di identificare in

modo automatico schemi di comportamento anomalo di utenti o di altre componenti dell'infrastruttura IT. Gli algoritmi a disposizione della piattaforma vengono addestrati a riconoscere gli schemi di comportamento abitualmente adottati dagli utenti e da altre entità in modo tale da riconoscere attività anomale e potenziali malintenzionati.

4.2.9 Reportistica

Il Fornitore predispone Report Tecnici periodici che indichino lo stato generale in ambito sicurezza dell'infrastruttura dell'organizzazione che lo ha richiesto.

Sono altresì richiesti Executive Report (Executive Summary) per fornire informazioni di tipo statistico da presentare ai vertici dell'organizzazione con periodicità concordata. Tali report considerano rischi, incidenti, malware, ed altro, rilevati in un certo periodo, prendendo in considerazione i KPI (Key Performance Indicator) definiti dall'Amministrazione e necessari al monitoraggio della sicurezza informatica.

4.2.10 Servizio di Digital Forensic

Il Fornitore fornisce figure professionali certificate e competenti per l'implementazione dei processi che consentano all'Amministrazione di organizzare e trattare in modo opportuno le informazioni presenti nei diversi dispositivi aziendali per la propria tutela a fronte di una richiesta di presentazione di prove in tribunale o funzionali a diverse tipologie di indagini specifiche. Oltre ai servizi di Analisi Forense eseguiti per motivi legali su copie dei dati e dei sistemi. L'Analisi delle prove deve essere effettuata con i software più utilizzati dalle forze dell'ordine e dalle agenzie di intelligence. Viene emesso un report finale che evidenzia tutte le attività di indagine effettuate, i risultati rilevati e le eventuali estrazioni di file di prova con allegata la relativa compilazione della catena di custodia, a fini investigativi anche da parte delle Autorità competenti.

4.2.11 Servizio di threat intelligence

Il Fornitore eroga servizi di Threat Intelligence per il monitoraggio delle più recenti informazioni relative a minacce, vulnerabilità ed exploit di sicurezza garantendo: accuratezza, affidabilità, chiarezza e completezza.

All'interno di tali servizi possono essere richiesti a titolo puramente indicativo e non esaustivo:

- APT feed: fornitura dei dati relativi ai più recenti IoCs (indicatori di compromissione);
- Threat sharing automatizzata;
- Asset tracker & data leak: rilevare fughe di dati di proprietà dell'Amministrazione in Internet, anche nel c.d. "dark web".

Le informazioni di maggior impatto devono essere comunicate tempestivamente al personale che effettua il monitoraggio, in tempo reale, dell'infrastruttura di sicurezza e ai referenti dell'organizzazione che ha richiesto il servizio.

- Il Fornitore dovrà mettere a disposizione una piattaforma web che permetta all'Amministrazione di accedere alle apposite dashboard che rendono disponibili le informazioni (Knowledge base).

4.2.12 Servizio di host hardening

Il Fornitore eroga un servizio di host hardening che consiste nel supporto all'amministrazione per la definizione, manutenzione ed il controllo di procedure e politiche di configurazione sicura, nonché di cancellazione sicura dei dati, e di aggiornamento dei sistemi server e storage, apparati di rete e sistemi client e mobile, considerando anche eventuali spostamenti in territori considerati non sicuri, in linea con policy di sicurezza adottate dall'Amministrazione che saranno condivise, con le figure professionali dell'IT, interno all'Ente, del Fornitore dei servizi di IT System Management o di eventuali altre figure professionali che operano per conto dell'Amministrazione.

4.2.13 Servizio di security awareness

Il Fornitore dovrà mettere a disposizione un sistema integrato con il quale eseguire simulazioni e testing e valutare conoscenze inerenti argomenti specifici sulla sicurezza informatica per i quali coinvolgere tutto il personale, oltre a quello IT. L'Amministrazione si riserva di poter valutare altri servizi alternativi che il Fornitore dovrà rendersi disponibile a proporre.

Il servizio richiesto deve essere erogato secondo criteri da stabilire con l'Amministrazione e, comunque, deve essere in grado di adattarsi dinamicamente alle esigenze dell'Amministrazione stessa, con metodologie di approccio innovative, indipendentemente dai contenuti. A titolo esemplificativo e non esaustivo, si possono elencare simulazioni di eventi di attacco di diversa tipologia e con modalità differenti di remediation, gestione di campagne di phishing massive e altre forme di sfida in modalità interattiva con diversi livelli di difficoltà che si rendessero particolarmente interessanti per migliorare le conoscenze nell'ambito.

Il servizio deve proporre aggiornamenti in grado di stare al passo con la rapida evoluzione delle tecniche di attacco e, conseguentemente, la creazione di nuove metodologie di difesa, che quindi devono essere ricomprese nel servizio offerto.

Come noto, infatti, il campo della sicurezza informatica si caratterizza per la rapidità con le quali si modificano le tecniche di attacco e conseguentemente la ricerca e sviluppo di metodologie di difesa, che devono essere ricomprese nelle simulazioni rivolte anche alle figure specialistiche

dell'Amministrazione come quelle citate, e che sono anche quelle ad essere le prime chiamate ad individuare e bloccare con efficacia gli attacchi mirati, e a risolvere rapidamente le violazioni sospette. È quindi fondamentale che il servizio sia nativamente predisposto alla flessibilità e adattabilità secondo le esigenze dell'Amministrazione in tempi rapidi ed adeguati alle esigenze del momento.

La forma di fruizione del servizio dovrà ricomprendere le licenze necessarie per l'erogazione dello stesso, incluso il supporto di gestione dei test di verifica del livello di preparazione raggiunto, oltre ai servizi di erogazione delle simulazioni suddette.

Le modalità di erogazione dei corsi devono essere strutturate in aderenza alle linee guida sull'accessibilità, le WCAG 2.1 (https://www.w3.org/Translations/WCAG21-it/) a livello A e AA.

4.2.14 CyberSecurity & Privacy Legal Advisor

Il Fornitore mette a disposizione la figura professionale del Cyber security and Privacy legal advisor che rappresenta il supporto in affiancamento al team Sicurezza e al Servizio Legale dell'Amministrazione e contribuisce alla valutazione e analisi dei rischi, alla stesura di procedure e disciplinari ed eventuali documenti programmatici relativi alla sicurezza, all'elaborazione e all'implementazione legale di un modello di sicurezza informatica e dei sistemi di gestione della sicurezza delle informazioni (ISMS) e agli aspetti legali collegati al verificarsi delle minacce di attacchi informatici, sia in fase di reazione all'evento e sia nella fase di elaborazione dell'incident response.

La consulenza e il supporto legale richiesto ricomprendono tutti gli aspetti connessi alla sicurezza fisica e logica, inclusi quelli relativi alle strumentazioni informatiche utilizzate dall'Amministrazione, quindi dai personal computer ai dispositivi mobili e ai server, le comunicazioni digitali, la videosorveglianza, ecc.

Gli aspetti sui quali si chiede la consulenza devono ricomprendere:

- Interruzione dell'attività clinico-sanitaria;
- Perdite economiche e finanziarie conseguenti ai danni post-incident;
- Furto di informazioni private e/o cliniche;
- Diffusione di informazioni private e/o cliniche;
- Supporto relativo agli adempimenti ed obblighi di notifica al Garante Privacy (data breach)
- Contenziosi connessi agli incidenti di sicurezza informatica;
- Implicazioni connesse al trattamento dei dati degli utenti;
- Verifiche sulla compliance rispetto le normative sulla sicurezza informatica;
- Danno reputazionale e di immagine.

La consulenza legale deve essere offerta sia per una gestione preventiva degli incidenti e sia post-incident e basarsi sulle norme principali note in ambito di sicurezza come: il regolamento europeo GDRP e s.m.i., le misure minime di sicurezza per le pubbliche amministrazioni dell'AGID, la Direttiva UE 2016/1148 (Direttiva NIS).

Deve inoltre fornire supporto alla gestione e coordinamento delle diverse figure professionali sia interne all'Amministrazione e sia esterne, tra cui l'Alta Direzione, il DPO, l'Ufficio Legale, il Servizio Informatico, l'Ufficio Comunicazione, eventuali Agenzie di assicurazione.

4.2.15 Servizio di security advisoring

Il Fornitore dovrà erogare un servizio di Security Advisoring per l'elaborazione e la pianificazione di attività di diagnostica e verifiche di sicurezza, anche periodiche, e relativi bollettini, utilizzando modalità e standard riconosciuti a livello nazionale ed internazionale. Il servizio dovrà prevedere tecniche di rilevamento ed analisi delle vulnerabilità in diversi ambienti, quali ad esempio a titolo esemplificativo e non esaustivo, applicativi aziendali sia web based e sia non web based, reti wired e wireless, sistemi operativi (tipicamente Microsoft e Debian/Linux) e DBMS.

Il Fornitore predispone, emette ed invia periodicamente bollettini di sicurezza volti a rappresentare una sintesi delle evidenze rilevate dal monitoraggio continuo delle fonti aperte e proprietarie, necessarie ad acquisire informazioni su nuove minacce e vulnerabilità e correlate con i sistemi presenti nell'infrastruttura dell'Amministrazione che ha richiesto il servizio di Monitoraggio in tempo reale di eventi di sicurezza al fine di valutare potenziali rischi.

Nel caso di eventi particolarmente critici e nel caso di una elevata esposizione al rischio che richiedano l'intervento con tempi di reazione ridotti, vengono inviate delle segnalazioni ad-hoc sia ai referenti tecnici dell'Amministrazione che ai referenti tecnici del SOC per verificare quali regole e correlazioni siano da applicare sui sistemi di monitoraggio, oltre alla verifica dei possibili eventuali rimedi da applicare a sistemi e reti, in collaborazione con le figure professionali dell'IT, interno all'Ente, del Fornitore dei servizi di System Management o di eventuali altre figure professionali che operano per conto dell'Amministrazione.

4.2.16 Servizi di Service e Performance Management

È compito del Fornitore assicurare che i servizi di gestione in ambito sicurezza informatica siano organizzati e strutturati secondo un approccio process-driven, in cui la complessa struttura organizzativa/operativa dei servizi sia scomposta in una serie di processi integrati e correlati tra loro in accordo con le best practices ITIL, con l'obiettivo, in ambito di sicurezza informatica, di:

- migliorare la qualità dei servizi;

- ridurre i costi di erogazione dei servizi;
- allineare i servizi con i bisogni correnti e futuri del business e dei clienti.

Nel caso in cui l'Amministrazione abbia già definito a priori la strutturazione dei processi di gestione secondo le best practices ITIL, il Fornitore dovrà erogare i servizi adottando i processi già definiti; nel caso in cui, invece, l'Amministrazione non abbia definito, in tutto o in parte, la strutturazione dei processi di gestione, il Fornitore dovrà, su richiesta e in accordo con l'Amministrazione, proporre e adottare un'adeguata strutturazione dei processi previsti.

Si ritiene utile sottolineare, in maniera più puntuale, il valore aggiunto atteso dall'operatività del Fornitore nell'ambito di alcuni tra i processi più significativi per l'evoluzione del modello di erogazione dei servizi.

Si precisa che non tutti i processi per cui ci si attende un impegno dal Fornitore sono di seguito elencati, fermo restando che il Fornitore deve supportare l'Amministrazione effettuando tutte le attività di competenza, sulla base di quanto stabilito nelle procedure operative che saranno rese disponibili o implementate nel corso della gestione contrattuale.

4.2.16.1 Gestione delle Richieste e delle Segnalazioni

In coerenza con i processi in uso presso l'Amministrazione, è richiesto che il Fornitore utilizzi gli strumenti resi disponibili dall'Amministrazione per tracciare le attività a carattere operativo nonché le richieste di informazioni e di segnalazione di disservizio.

In particolare, il Fornitore stesso deve:

- alimentare gli strumenti di tracciatura;
- effettuare la ricezione e la presa in carico delle richieste nei tempi concordati;
- aggiornare le informazioni di ciascun ticket con l'effettivo stato/andamento delle attività;
- fornire una stima dei tempi di esecuzione e una diagnosi relativa all'intervento da effettuare;
- effettuare la chiusura dei ticket;
- gestire, per quanto di competenza, gli interventi dei fornitori terzi.

4.2.16.2 Supporto al Processo di Incident e Problem Management

Al fine di garantire la corretta fruizione dei servizi da parte dell'utenza di riferimento, il Fornitore è responsabile della gestione di tutti i casi in cui sia rilevabile una interruzione o un degrado nella fruizione del servizio. Tale responsabilità è indipendente dalla causa dell'interruzione/degrado, che può essere legato al software, all'hardware e relativo firmware sistemi e/o apparati di sicurezza.

Il Fornitore è tenuto ad effettuare le attività necessarie al ripristino del servizio all'utenza di riferimento entro i tempi massimi prefissati, anche attraverso l'attivazione delle procedure di escalation concordate.

Tali procedure tengono conto del livello di gravità del malfunzionamento e dell'impatto dello stesso sull'operatività dell'utenza.

L'attività di gestione dei malfunzionamenti deve essere sia proattiva, ossia rivolta alla prevenzione, sia reattiva, ossia rivolta alla gestione ed infine alla risoluzione di tutti gli eventi che comportano l'interruzione o il degrado nella fruizione del servizio.

Pertanto, tra le attività richieste si includono:

- l'identificazione del malfunzionamento, la sua documentazione, la gestione delle comunicazioni e dell'escalation e la sua risoluzione, anche attraverso l'attività di terze parti;
- l'analisi del verificarsi di problemi ripetitivi. I risultati dell'analisi sono inseriti nella knowledge base e sugli elementi interessati sono eseguiti controlli approfonditi atti ad individuare e risolvere problemi di tipo strutturale, secondo quanto concordato con la l'Amministrazione nell'ambito del processo di Problem management;
- l'analisi delle informazioni derivanti dall'esecuzione delle attività di verifica di performance dei sistemi, tenendo conto delle informazioni provenienti dai sistemi di monitoraggio.

In ultimo, è responsabilità del Fornitore il salvataggio dei dati ai fini dell'analisi di incidenti di sicurezza. Il Fornitore deve assicurarsi che i sistemi, anche non direttamente gestiti, inviino al sistema di Log Management le informazioni utili alle attività di analisi da parte del SOC, attivando - in caso negativo - le procedure concordate con l'Amministrazione.

È richiesto, infatti, che sia effettuata la conservazione di tutti i log di auditing relativi sistemi e apparati di sicurezza e quanto altro possa essere necessario alla ricostruzione di comportamenti insidiosi e per l'individuazione di possibili responsabilità penali e civili conseguenti a condotte illecite. Tali log devono essere mantenuti in linea per il periodo concordato con l'Amministrazione. Su tali log l'Amministrazione si riserva di richiedere al team di effettuare ricerche ed elaborazioni statistiche puntuali.

Si precisa che i dati da raccogliere e da salvare ai fini dell'indagine sugli incidenti di sicurezza saranno concordati successivamente all'avvio della fornitura.

4.2.16.3 Supporto al Processo di Change e Release & Deployment Management

Al fine di garantire il corretto funzionamento, lo sviluppo e l'evoluzione dell'infrastruttura ICT dell'Amministrazione, il Fornitore è responsabile della pianificazione, dell'attuazione, del tracciamento e della verifica dei cambiamenti dell'hardware, del firmware, dell'evoluzione dei

sistemi operativi, dei prodotti di sicurezza informatica e delle relative correzioni coerentemente con i processi di Change Management e Release & Deployment Management.

4.2.16.4 Supporto al Processo di Service Asset & Configuration Management

Il Fornitore deve garantire il costante, accurato e continuo allineamento delle basi dati del CMDB; nel caso in cui tali aggiornamenti non possano essere eseguiti automaticamente, il Fornitore deve procedere con l'aggiornamento manuale. Si precisa che l'aggiornamento del CMDB è prevalentemente effettuato in automatico attraverso prodotti di scansione le cui politiche sono definite dall'Amministrazione e sono supportati da script/procedure automatiche che potrebbero essere realizzate da terzi.

Si precisa che i processi e le procedure operative sono oggetto di revisione e miglioramento continuo, pertanto, nel periodo contrattuale, le modalità indicate potrebbero variare. In ogni caso i fornitori sono obbligati a seguire qualsiasi variazione dei processi e delle procedure operative che l'Amministrazione indicherà.

L'aggiornamento costante e accurato della baseline, in particolare del CMDB, è ritenuto il nucleo fondamentale sui cui si fondano:

- i processi già in uso nonché i processi che potrebbero essere eventualmente adottati ed implementati nel corso della durata contrattuale;
- il patrimonio informativo relativo alla consistenza e alla configurazione dell'infrastruttura ICT dell'Amministrazione;
- la valutazione di eventuali impatti per i servizi di business dell'Amministrazione a fronte di evoluzioni, cambiamenti di carattere infrastrutturale;
- le analisi volte all'integrazione e/o all'introduzione di nuovi servizi a supporto dell'attività istituzionale dell'Amministrazione;
- la rilevazione e la misurazione della qualità del servizio all'utenza di riferimento.

Si ritiene utile precisare che, alla data di inizio attività, il CMDB potrebbe non essere completo di tutte le informazioni previste.

Ad inizio fornitura, è richiesto al Fornitore un security assessment per la verifica sulla postura di sicurezza oltre alla verifica sulla consistenza e coerenza dei dati di Asset & Configuration, degli Utenti Amministratori e delle relazioni tra gli stessi.

4.2.16.5 Supporto al Processo Capacity Management

Il Fornitore è responsabile dell'esecuzione delle attività operative a supporto del processo di Capacity Management. Pertanto, è responsabile della raccolta dei dati, dell'analisi periodica dello stato di

salute dell'Infrastruttura ICT, in ambito sicurezza informatica, affidata in gestione, dell'analisi dei trend di carico e della produzione di reportistica che mostri la situazione riassuntiva di ciascun sistema e che ne evidenzi eventuali criticità o necessità di evoluzione.

Si precisa che l'Amministrazione si riserva di richiedere la produzione di ulteriore reportistica il cui contenuto, formato e periodicità è concordato ad inizio fornitura ed eventualmente rivisto, nel corso della durata dei servizi, ai fini della predisposizione del Piano della Capacità.

Il Fornitore, nell'erogazione del servizio, può utilizzare gli strumenti e i prodotti resi disponibili dall'Amministrazione ovvero può utilizzare script e/o le funzionalità native del software di sistema.

4.2.16.6 ServiceDesk Sistemistico di Sicurezza Informatica

Nell'ambito dei processi strutturati di Service Management, il Fornitore deve prevedere una funzione di Service Desk Sistemistico di sicurezza informatica, che agisca come punto di contatto tra i referenti informatici dell'Amministrazione e l'IT Security Management, per gestire incidenti e richieste degli utenti e fornire un'interfaccia per gli altri processi, tra cui Change, Problem, Configuration, Release, gestendo tutto il ciclo di vita dell'incidente, assieme alle figure professionali preposte, o della service request.

Gli elementi distintivi della funzione di Service Desk Sistemistico sono:

- prima diagnosi e tentativo di risoluzione delle segnalazioni/richieste al primo livello, anche attraverso l'utilizzo delle informazioni presenti nella Knowledge base;
- classificazione degli incidenti o richieste, attraverso modalità' obiettive per classificare gli incidenti in modo che siano assegnati opportunamente;
- assegnazione della priorità, attraverso modalità obiettive per l'assegnamento della priorità di un incidente (ad esempio attraverso una matrice di impatto/urgenza);
- assegnazione degli incidenti/richieste, automatizzando il più' possibile il routing dei casi in base al workload e alle competenze di ogni tecnico, in modo da ottimizzare le risorse;
- assegnazione a gruppi esterni, attraverso accordi con Fornitori terzi responsabili di specifiche attività.
    - La funzione di service desk sistemistico è relativa alle problematiche di system management dei sistemi di sicurezza informatica descritte nel presente Capitolato Tecnico e ha come principale utenza di riferimento i referenti informatici dell'Amministrazione. E' compresa l'assistenza agli utenti per problematiche che riguardano specifici incidenti di sicurezza che coinvolgono le postazioni di lavoro e gli utenti medesimi.

5. LOTTI 1 - 2. MODELLI DI EROGAZIONE E REMUNERAZIONE DEI SERVIZI

Nei capitoli precedenti i servizi di System Management e Sicurezza Informatica sono descritti e classificati dettagliatamente in base ai contenuti e alle specificità tecniche di ciascuno. In questo capitolo, invece, tali servizi sono sintetizzati e classificati in macrocategorie organizzate dal punto di vista dei modelli di erogazione e di remunerazione piuttosto che da quello dei contenuti tecnici. Tali modelli costituiscono la base per il dimensionamento dei servizi e per la formulazione delle offerte economiche. Le modalità di erogazione /remunerazione e la misura del canone annuo sono riepilogate nelle tabelle seguenti:

Lotto 1

Macro Categoria	Modalità di erogazione/remunerazione	Il canone annuo corrisponde al prezzo per
Servizio di monitoraggio NOC	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi e Apparati di rete;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi mail server;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi DB server;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi Web server;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi Back office;	Canone annuo	Server/Appliance (virtuale o fisico)
Sistemi Storage backup;	Canone annuo	Server/Appliance (virtuale o fisico)
Figure Professionali:		
TEM - ICT Operation Manager;	GG/uomo	
CET - Enterprise Architect;	GG/uomo	
SPP - System Architect;	GG/uomo	
SIS - System Administrator Senior;	GG/uomo	
SIM - System Administrator Middle;	GG/uomo	
SIJ - System Administrator Junior;	GG/uomo	

DBS - Database Administrator Senior;	GG/uomo	
DBJ - Database Administrator Junior;	GG/uomo	
SRS - Network Specialist Senior;	GG/uomo	
SRJ - Network Specialist Junior.	GG/uomo	

Lotto 2

Macro Categoria	Modalità di erogazione/remunerazione	Il canone annuo corrisponde al prezzo per
Servizio di monitoraggio SOC	Canone annuo	FASCIA DI EPS*
Sistemi Firewall, IDS,IPS	Canone annuo	PIATTAFORMA**
Sistemi Antivirus e di telemetria xDR/EDR/NDR	Canone annuo	PIATTAFORMA**
Sistemi WAF,	Canone annuo	PIATTAFORMA**
Sistemi SIEM, SOAR,	Canone annuo	PIATTAFORMA**
Servizio di Incident response & remediation		ENTE ***
Servizio di threat intelligence / APT-feed / asset tracker & data leak	Canone annuo	DOMINIO
Servizio di User and entity behavior analytics (UEBA)	Canone annuo	UTENTE
Servizio di host hardening	Canone annuo	DEVICE MODEL****
Servizio di security awareness	Canone annuo	UTENTE
Servizio di Vulnerability Management	Canone annuo	IP
Servizio di Application Security Testing	Canone annuo	APPLICAZIONE
Figure Professionali:		
Security Project Manager	GG/uomo	
Governance & risk compliance (GRC) consultant	GG/uomo	
Security architect & engineer	GG/uomo	
Security Advisor senior	GG/uomo	
Security Advisor junior	GG/uomo	
Security specialist	GG/uomo	
Security specialist con reperibilità H24	GG/uomo	
Security Analyst senior	GG/uomo	
Security Analyst junior	GG/uomo	
Vulnerability researcher / Ethical Hacker senior	GG/uomo	

Vulnerability researcher / Ethical Hacker junior	GG/uomo	
Incident handler / response senior	GG/uomo	
Incident handler / response junior	GG/uomo	
Digital forensic	GG/uomo	
CyberSecurity & Privacy Legal Advisor	GG/uomo	

Note:

*Per le Fasce di EPS vedere in calce al paragrafo 5.1 seguente;

** Per Piattaforma si intende un'infrastruttura costituita da componenti hardware e software per l'erogazione di servizi informatici tramite interfacce applicative e funzionalità specifiche;

*** Sono inclusi fino ad un massimo di 3 incidenti e 5 segnalazioni all'anno;

****Per Device Model si intende la tipologia del dispositivo ovvero una aggregazione di device.

5.1 Servizi a Canone

Nell'ambito della presente Convenzione sono definite due distinte modalità di presidio del servizio: **"Presidio on-site"** o **"Presidio da remoto"** corrispondenti ad un servizio erogato da personale del Fornitore allocato fisicamente nella sede dell'Amministrazione nel primo caso, presso il Centro Servizi del Fornitore nel secondo caso, con l'utilizzo di strumenti che potranno essere quelli del fornitore o quelli dell'Amministrazione secondo le esigenze dell'Amministrazione stessa e che saranno oggetto di valutazione in fase di assessment.

Il "**Servizio di monitoraggio sistemi e reti**" comprende i servizi di monitoraggio dei sistemi per la rilevazione di malfunzionamenti hardware e/o software, gli interventi di primo livello e le attività di escalation verso i livelli superiori a seguito di procedure schedulate.

Il servizio può essere erogato sia in modalità di presidio on site che in modalità remota dal Centro Servizi del Fornitore.

Il **"Servizio di Monitoraggio in tempo reale di eventi di sicurezza**" comprende tutte le attività di monitoraggio dell'infrastruttura IT dell'Amministrazione al fine di rilevare e gestire in tempo reale gli eventi relativi alla sicurezza informatica.

Il servizio può essere erogato sia in modalità di presidio on site che in modalità remota dal Centro Servizi del Fornitore. La "**conduzione operativa sistemi**", la "**conduzione operativa reti**" e la "**conduzione operativa di apparati e sistemi di sicurezza"** comprende in generale tutti i **servizi**

base di gestione di tipo continuativo svolti nell'orario base di lavoro, includendo gestione e configurazione sistemi e reti, manutenzione sistemi, gestione software di base e di ambiente e basi dati, descritti nel lotto 1; gestione e configurazione manutenzione apparati e sistemi sicurezza, descritti nel lotto 2.

I servizi di "**Monitoraggio sistemi e reti**", "**Monitoraggio in tempo reale di eventi di sicurezza"** e "**Conduzione operativa**" possono essere erogati sia in modalità di presidio on site che in modalità remota dal Centro Servizi del Fornitore, a seconda delle preferenze dell'Amministrazione.

La **remunerazione dei servizi è a canone** ed è basata sulla dimensione e le caratteristiche dell'infrastruttura tecnologica oggetto del servizio stesso, ovvero è indipendente dal numero e dalla tipologia di risorse professionali impiegate dal Fornitore.

Nel caso specifico dei servizi di Monitoraggio (NOC e SOC) e conduzione operativa, oltre alle fasce orarie di erogazione del servizio, concorre alla formazione del canone anche la classificazione dei sistemi ed il livello di criticità ed eventualmente, come nel caso della conduzione operativa, la reperibilità come meglio definito di seguito.

Inoltre, per il servizio di Monitoraggio SOC (Lotto 2) il canone è differenziato nelle seguenti fasce in base al numero di EPS (eventi per secondo):

- fino a 1.000 EPS;
- da 1.001÷5.000 EPS;
- da 5.001÷10.000 EPS;
- da 10.001 EPS in su,

sia per il servizio con ORARIO BASE che per il servizio con ORARIO CONTINUATO.

5.1.1 Orari del servizio

L'effort dedicato alle attività di monitoraggio sistemi, conduzione operativa dei sistemi, delle reti, della sicurezza informatica e reperibilità standard varia in base all'orario di servizio richiesto al Fornitore. Per tale motivo, nell'ambito della presente Convenzione si definiscono, ove previste, per il **Lotto 1** tre fasce orarie di riferimento:

Finestra di erogazione dei servizi Sistemistici		
Orario BASE	**Orario ESTESO**	**Orario CONTINUATO**
Lun-Ven 8.00 – 18.00	Lun-Ven 7.30 – 19.00; Sab 7.30 - 14.00	H24, 7 giorni su 7

Per il **Lotto 2**:

Finestra di erogazione dei servizi Sicurezza informatica

Orario BASE		Orario CONTINUATO
Lun-Ven 8.00 – 18.00		H24, 7 giorni su 7

5.1.2 Classificazione dei sistemi, livello di criticità e livello di severità

Le tipologie di Sistemi oggetto della presente fornitura corrispondono a:

Lotto 1:

Sistemi Mail Server
Sistemi DB Server
Sistemi Application Server / Web Server / Middleware
Sistemi infrastrutturali/backoffice

Lotto 2:

Sistemi Firewall, IDS/IPS;
Sistemi Antivirus e di telemetria (xDR/EDR/NDR);
Sistemi WAF;
Sistemi SIEM, SOAR;

In particolare, per quanto attiene alla classificazione per **livello di criticità** in ambito IT System Management (Lotto 1) si intende:

◦ **Sistema non critico**: disponibilità =< 99,8%, tempo di presa in carico malfunzionamenti entro 4 ore, ambiente di produzione, sistemi di test/sviluppo o sistemi che comunque non impattano in modo significativo sui processi di business dell'Ente*;*

◦ **Sistema Business critical**: disponibilità > 99,8%, tempo di presa in carico malfunzionamenti entro 2 ore, ambiente di produzione, tipicamente sistemi che impattano in modo significativo sui processi di business dell'Ente*;*

◦ **Sistema Mission critical**: disponibilità > 99,8%, tempo di presa in carico malfunzionamenti entro 1 ora, ambiente di produzione tipicamente sistemi il cui malfunzionamento blocca i processi di business dell'Ente.

Inoltre, posto che tutti i sistemi di sicurezza (Lotto 2) sono considerati con il livello di criticità "Sistema Mission Critical" e pertanto deve essere garantita la disponibilità di cui sopra, per l'operatività di apparati e sistemi, nonché per la gestione degli incidenti di sicurezza gestiti dal SOC e dal Incident Response and Remediation Team (IRRT), deve essere considerata la seguente **classificazione per severità** in base alla quale la presa in carico del disservizio o dell'incidente deve essere effettuata entro gli SLA indicati in tabella 5 o in tabella 6 e tabella 7:

◦ **BASSA**:

- impatto ridotto sull'operatività di un servizio o un sistema di sicurezza in ambiente di

produzione, test/sviluppo;

- incidente derivante da un possibile rischio di minacce da virus o malware oppure dall'intrusione da parte di utenti non autorizzati oppure che provoca la parziale inattività di un esiguo numero di utenti autorizzati;

◦ **MEDIA**:

- impatto che degrada e rende parzialmente interrotto un servizio o un sistema di sicurezza in ambiente di produzione;
- incidente che compromette e degrada le prestazioni o il parziale funzionamento di reti, sistemi e applicazioni oppure che provoca la parziale inattività di un significativo gruppo di utenti autorizzati;

◦ **ALTA**:

- impatto grave sull'operatività e sul livello di compromissione di un servizio o di un sistema di sicurezza in ambiente di produzione;
- grave incidente di sicurezza a causa di sistemi compromessi, accessi abusivi, rischio frodi e furti di dati dell'Amministrazione, estesa infezione da parte di virus e malware, perdita di immagine e/o reputazionale.

I suddetti criteri di classificazione concorrono all'individuazione dei canoni annui (la cui applicazione deve essere definita dall'Amministrazione nella fase di assessment iniziale, vedasi paragrafo 7.1) e/o dei relativi SLA.

5.1.3 Reperibilità ed interventi fuori orario

Reperibilità standard

Il modello di remunerazione previsto per il servizio di reperibilità standard è basato su un canone annuale complessivo calcolato in base ai valori scelti per le variabili già descritte nel dettaglio al paragrafo 5.1.2.

Reperibilità individuale

Per le attività di conduzione operativa e di supporto specialistico di tipo continuativo, l'Amministrazione può richiedere la reperibilità, al di fuori del normale orario di lavoro, del personale già impegnato nelle attività onsite, per rispondere tempestivamente ad eventuali situazioni critiche. Per tale servizio, il modello di remunerazione è strettamente dipendente dal numero e tipologia di risorse professionali impiegate nell'erogazione del servizio stesso, pertanto viene prevista una remunerazione differente per la reperibilità di ciascuna figura professionale.

La singola Amministrazione, sulla base delle proprie esigenze, definirà gli impegni per la reperibilità complessivamente richiesti, in termini di giornate uomo per figura professionale.

Intervento on site fuori orario

Per le attività di conduzione operativa e di supporto specialistico, l'Amministrazione può richiedere interventi onsite al di fuori del normale orario di lavoro a seguito di malfunzionamenti o eventi collegati alla sicurezza informatica, oppure estensioni temporanee dell'orario di servizio per esigenze contingenti di durata limitata nel tempo che richiedano la piena disponibilità del personale di conduzione e/o di supporto oltre l'orario standard.

5.2 Supporto Specialistico

Il servizio di "supporto specialistico" comprende due modalità di erogazione dei servizi sistemistici e di sicurezza informatica, che sono strettamente dipendenti dal numero e tipologia di risorse professionali impiegate dal Fornitore nell'erogazione dei servizi stessi:

- attività di supporto continuativo;
- attività di supporto a richiesta.

Si richiede, infine, che le risorse impegnate ad erogare il supporto specialistico, in loco o da remoto, possano interagire con in Centri di Competenza del Fornitore, a titolo esemplificativo (e non esaustivo) si elencano alcuni possibili Centri di Competenza:

- Centri di Competenza su Tecnologie SAP;
- Centri di Competenza su Tecnologie OpenSource;
- Centri di Competenza su Tecnologie Cloud e Virtualizzazione;
- Centri di Competenza su Tecnologie Storage;
- Centri di Competenza su Tecnologie Database;
- Centri di Competenza su Tecnologie Firewall, IDS/IPS, Antivirus e xDR/EDR/NDR;
- Centri di Competenza su Tecnologie WAF;
- Centri di Competenza di Tecnologie SIEM, SOAR.

5.2.1 Attività di supporto continuativo

Tali attività rientrano nell'ambito generale delle attività di gestione e sviluppo sistemi ma, per i motivi tecnici e/o organizzativi, non possono essere ricomprese nel modello dei servizi di conduzione operativa, e si configurano quindi come affiancamento al personale dell'Amministrazione e/o al personale del Fornitore impiegato nei servizi di conduzione.

I motivi tecnici alla base della necessità di supporto specialistico continuativo possono ad esempio derivare dalla necessità di effettuare attività che richiedono specifiche competenze in ambiti

particolari (ad esempio team di analisi delle politiche di sicurezza).

I motivi organizzativi possono invece essere relativi, ad esempio, ai casi in cui le attività di conduzione operativa sono effettuate direttamente da personale dell'Amministrazione e il personale del Fornitore è di supporto a quello dell'Amministrazione e opera di concerto con quest'ultimo e sotto il suo controllo diretto. In questo caso le attività e le responsabilità suddette sono anche a carico dell'Amministrazione, quindi, la responsabilità del Fornitore è limitata ed è generalmente orientata a garantire la disponibilità e l'operatività delle risorse impiegate.

La durata minima del servizio di supporto specialistico continuativo è annuale e sono incluse eventuali sostituzioni per ferie e malattia del personale. Per quanto riguarda la modalità di presidio è di tipo onsite. La singola Amministrazione, sulla base delle proprie esigenze, definirà le attività di supporto continuativo richieste, in termini di numero e tipologia di figure professionali, che saranno quantificate. Il modello di remunerazione, per il servizio, è a GG/uomo.

5.2.2 Attività di supporto a richiesta

Tali attività comprendono:

- attività di supporto specialistico con affiancamento al personale dell'Amministrazione e/o al personale di conduzione operativa, che possono essere richieste ed erogate in modalità estemporanea (pur nell'ambito di un'opportuna pianificazione), per durate variabili e per periodi non contigui. La remunerazione del servizio è a "GG/uomo" ed è dipendente dal numero e dalla tipologia di risorse professionali richieste al Fornitore.
- attività di sviluppo/evoluzione delle infrastrutture tecnologiche definite in termini temporali (inizio e fine attività) e con specifici prodotti di output. Tali attività riguardano modificazioni significative dell'ambiente elaborativo, che richiedono un effort elevato ma limitato nel tempo, per le quali non ci si può avvalere del servizio di conduzione operativa, né del servizio di supporto continuativo. La remunerazione del servizio è "GG/uomo" ed è basata sull'effort stimato ad inizio attività, ovvero sul numero e sulla tipologia di risorse professionali previste;

Per le tipologie di attività suddette, l'orario di lavoro di riferimento per una singola risorsa professionale è di 8 ore al giorno.

Per le attività di supporto specialistico con affiancamento al personale dell'Amministrazione e/o al personale di conduzione operativa, la modalità di presidio è di tipo onsite.

Le attività di supporto specialistico a richiesta sono svolte dalle Figure professionali riportate nell'Allegato A al presente Capitolato.

5.3 Modalità di attivazione ed esecuzione della fornitura

Le risorse che verranno impiegate nelle attività devono essere di gradimento dell'Amministrazione, e devono avere i requisiti di professionalità richiesti e dichiarati dal Fornitore; l'Amministrazione si riserva la facoltà di ricusare detto personale per giustificati motivi.

È facoltà dell'Amministrazione verificare in via preventiva le competenze tecnico-professionali del personale specialistico proposto.

I controlli e le verifiche del personale effettuati dall'Amministrazione non liberano il Fornitore dagli obblighi e dalle responsabilità inerenti al contratto.

Competeranno all'Amministrazione la supervisione ed il controllo delle prestazioni rese dal personale inviato dal Fornitore per l'adempimento dei servizi ordinati.

5.4 Documentazione

Le attività richieste comportano la stesura e l'aggiornamento di tutta la documentazione necessaria secondo gli standard adottati dall'Amministrazione. La documentazione degli interventi eseguiti riguardanti attività tecniche o progettuali è da intendersi parte integrante della fornitura e dovrà essere consegnata in formato elettronico secondo la pianificazione concordata.

La documentazione tecnico-specialistica relativa ad interventi ed attività eseguite è a carico del Fornitore e deve essere prodotta utilizzando strumenti di gestione documentale e di reporting forniti dall'Amministrazione; strumenti alternativi potranno essere proposti dal Fornitore nell'offerta tecnica. In ogni caso l'Amministrazione si riserva di sottoporli a verifica ed eventualmente accettarli in fase di avviamento della fornitura. Per l'utilizzo di eventuali prodotti aggiuntivi non è previsto alcun corrispettivo.

5.5 Orario e luogo di lavoro

Le prestazioni oggetto del presente capitolato si svolgeranno nella modalità on-site presso gli uffici dell'Amministrazione (anche con utilizzo di una strumentazione di supporto messa a disposizione dall'Amministrazione stessa) o da remoto presso il Centro Servizi del Fornitore.

Tali prestazioni saranno erogate nelle fasce orarie previste dalle singole Amministrazioni in sede di contratto.

5.6 Avvicendamento contrattuale

Al fine di rendere il più efficace possibile l'avvicendamento contrattuale, dopo l'emissione di un ordinativo di fornitura da parte di una Pubblica Amministrazione aderente alla Convenzione, il Fornitore dovrà rendere disponibili entro 5 giorni lavorativi le risorse necessarie al passaggio di

consegne dall'attuale Fornitore del servizio. La tipologia di figure professionali, il loro numero e le modalità di esecuzione di tale passaggio dovranno essere concordate con l'Amministrazione e comunque entro e non oltre 3 mesi. La presa in carico di tale know-how dovrà avvenire a titolo non oneroso per l'Amministrazione.

Entro il termine della fornitura, il Fornitore dovrà essere disponibile a trasferire il know-how acquisito all'Amministrazione o a terzi dalla stessa designati. Tale attività sarà remunerata secondo le tariffe del contratto allora vigente.

6. LOTTI 1 - 2. CARATTERISTICHE DELLE FIGURE PROFESSIONALI

6.1 Figure professionali

Si rinvia all'Allegato A – Figure professionali al presente Capitolato.

7. LOTTI 1 - 2. SERVIZIO DI ASSESSMENT E DI DEFINIZIONE DEL PIANO DI ESECUZIONE DEI SERVIZI

I servizi di Assessment e di definizione del Piano di Esecuzione dei Servizi sono volti all'esatta definizione tecnica, economica e gestionale del perimetro dei servizi oggetto del Contratto di Fornitura. Essi sono svolti dal Fornitore sia nella fase preliminare all'eventuale stipula del Contratto di Fornitura, sia nel corso dello stesso.

7.1 Assessment

Con l'Assessment, il Fornitore, anche sulla base della classificazione di cui al punto 5.1.2, individua le caratteristiche:

- dei sistemi da gestire/manutenere e, per ciascuno di essi, le caratteristiche che ne determinano il prezzo di gestione/manutenzione;
- dell'Amministrazione, dal punto di vista dell'organizzazione e delle procedure interne, al fine di definire e personalizzare le modalità e i processi di esecuzione dei servizi.

Il servizio si compone di:

- sopralluoghi, effettuati dai tecnici del Fornitore che effettueranno una ricognizione "fisica" presso le sedi dell'Amministrazione al fine di raccogliere le "informazioni di dettaglio" degli apparati da gestire ed eventualmente manutenere;
- raccolta di tutte le ulteriori informazioni relative alla configurazione software ed hardware dei suddetti apparati, necessarie o comunque utili all'efficace erogazione dei servizi;
- raccolta delle informazioni relative agli aspetti logistici, organizzativi e procedurali dell'Amministrazione, pure necessarie o utili all'efficace erogazione dei servizi;

Le attività saranno svolte dal Fornitore non solo a seguito delle predette richieste, ma nel corso dell'intera durata del Contratto di Fornitura, allo scopo di:

- rendere disponibile e mantenere aggiornata una base informativa completa e dettagliata del parco macchine in servizio presso l'Amministrazione e delle relative configurazioni hardware e software;
- adattare/ottimizzare modalità e processi di erogazione dei servizi ai mutati aspetti organizzativi e procedurali dell'Amministrazione.

Con il Security Assessment il Fornitore può verificare il livello di maturità della postura di sicurezza informatica dell'Amministrazione coinvolta. I controlli da applicare devono basarsi sul Framework Nazionale di Cyber Security (FNCS).

Il servizio si compone nel:

- predisporre la checklist (ove sia necessario), definire i referenti e il piano di interviste;
- essere di supporto all'organizzazione nell'effettuare le interviste, nel compilare la checklist ed eseguire la raccolta documentale;
- analizzare i dati;
- identificare e definire la postura iniziale e di riferimento al fine di predisporre un report di valutazione da presentare all'alta direzione dell'organizzazione e per definire il perimetro necessario ed utile all'efficace erogazione dei servizi.

Le attività saranno svolte dal Fornitore non solo per la fase iniziale ma anche nel corso dell'intera durata del contratto di fornitura con periodicità concordata allo scopo di:

- identificare le iniziative di sicurezza raccomandate;
- predisporre piani di sviluppo che permettano di migliorare il livello di sicurezza.
- supportare l'organizzazione per la predisposizione dell'analisi dei rischi, del trattamento del rischio e del piano di rientro.

Le attività potranno essere erogate dal Fornitore:

- in loco, contestualmente all'esecuzione dei sopralluoghi, o nel corso dell'esecuzione del Contratto di Fornitura;
- e/o con modalità automatizzate per la rilevazione dei componenti hardware e software, da riscontrare poi in loco in funzione della completezza dello strumento di discovery utilizzato e/o delle risultanze emerse;
- e/o fornendo all'Amministrazione indicazioni puntuali e dettagliate su come reperire e inviare al Fornitore le informazioni richieste, limitatamente a quelle di facile reperimento, e da

riscontrare comunque in loco in caso di dati dubbi.

Tutte le informazioni raccolte dal Fornitore e relative agli apparati dell'Amministrazione, dovranno essere memorizzate nel "Data Base degli Asset", base di dati centralizzata del Fornitore. Tale DB dovrà essere aggiornato a fronte di ogni evento che abbia impatto sulle informazioni stesse (es: interventi, installazioni/aggiornamenti HW e SW).

Con riferimento alle attività di conduzione degli apparati dell'Amministrazione, il Fornitore dovrà preliminarmente individuare gli eventuali:

- apparati che, alla data prevista per l'Avvio dei Servizi, risulteranno "End Of Support" da parte del Produttore;
- verificare se sia già nota la futura data di "End Of Support" dell'apparato e, in caso contrario, formulare le proprie previsioni basate sul ciclo di vita di apparati di stessa tipologia e produttore.

7.2 Piano di Esecuzione dei Servizi

Il Piano di Esecuzione dei Servizi dovrà contenere:

Risultati dell'Assessment

- Elenco, degli apparati oggetto della prestazione dei servizi di gestione ed eventualmente manutenzione, con le caratteristiche rilevanti ai fini della definizione tecnico/economica dei servizi stessi;
- Elenco degli apparati per i quali il Fornitore si avvale della facoltà di non prestare il servizio di gestione e/o manutenzione (apparati che risultino "End of Support" alla data di avvio dei servizi);
- Evidenza degli aspetti logistici, organizzativi e procedurali peculiari dell'Amministrazione, significativi ai fini della definizione delle modalità e dei processi di erogazione dei servizi.

Piano Tecnico-Organizzativo

- Esatta definizione tecnica dei servizi e delle modalità di erogazione tra cui:
  - descrizione delle attività che saranno svolte da remoto, con indicazione degli strumenti utilizzati e delle eventuali configurazioni e/o installazioni di software sugli apparati dell'Amministrazione;
  - descrizione delle attività che saranno svolte con indicazione della frequenza programmata;
- Definizione dei processi che regoleranno l'esecuzione dei servizi, relativamente alle attività:
  - di ordinaria gestione/manutenzione (monitoraggio apparati, interventi di manutenzione preventiva, etc.);
  - eseguite a seguito di specifiche richieste dell'Amministrazione;

  - scaturite da richieste di assistenza o segnalazione di malfunzionamenti, con descrizione dell'iter di escalation;
  - di change management, con riferimento alle politiche ed ai processi di change e alle procedure di ripristino;
  - di terze parti (fornitori di servizi di connettività, fornitori incaricati della gestione/assistenza/manutenzione di apparati nell'ambito di contratti preesistenti, etc.);
- Attività e tempistiche per l'Avvio dei servizi, con particolare riferimento alle attività di:
  - presa in carico degli apparati e start up dei servizi, con indicazione di quali saranno svolte in loco;
  - configurazione apparati e/o installazione software per la gestione da remoto;
  - migrazione da precedenti contratti e sistemi di gestione;
- Identificazione del Personale del Fornitore, che, in aggiunta al Referente locale, sarà coinvolto nell'esecuzione del Contratto Attuativo, con particolare riferimento alle risorse che effettueranno attività in loco.

Piano Economico

Il Piano Economico dovrà determinare, analiticamente, il costo di ciascuno dei servizi oggetto del Piano, per l'intera durata del Contratto di Fornitura, in conformità all'Offerta Economica, all'assessment e alla definizione del perimetro dei servizi di cui sopra, alle modalità di erogazione dei servizi e alla determinazione degli importi per i singoli servizi.

Il Piano Economico dovrà contenere inoltre l'importo complessivo dei servizi, suddiviso in:

- Importo complessivo dei servizi a canone (conduzione operativa, manutenzione, presidio, etc.);
- Importo forfettario complessivo dei servizi a consumo (GG/uomo) indicato in maniera presuntiva, e non vincolante per l'Amministrazione, che si vedrà fatturare, per i citati servizi, unicamente gli importi relativi ai servizi effettivamente utilizzati.

Su iniziativa del Fornitore, qualora le evidenze della gestione contrattuale suggeriscano l'opportunità di apportare modifiche ai processi e alle modalità di erogazione dei servizi – nel rispetto sempre di quanto previsto nel presente Capitolato e nell'Offerta Tecnica del Fornitore – tali da rendere i servizi più efficaci al contesto specifico dell'Amministrazione, il Piano di Esecuzione dei Servizi potrà essere aggiornato.

Nel caso in cui il Piano di Esecuzione dei Servizi sia aggiornato su richiesta dell'Amministrazione, qualora quest'ultima sia interessata ad estendere il perimetro dei servizi e/o degli apparati su cui prestare i servizi, il Piano Economico dovrà indicare esplicitamente la variazione degli importi

complessivi rispetto a quelli relativi al precedente Piano approvato. Laddove il Piano di Esecuzione dei Servizi aggiornato sia accettato dall'Amministrazione, tale variazione sarà pari all'importo del relativo Ordinativo Collegato.

8. LOTTI 1 - 2. OSSERVANZA DI NORME, LEGGI E REGOLAMENTI

Il Fornitore è tenuto all'osservanza delle norme di legge e di regolamento adottate dalle Autorità competenti in materia di contratti di lavoro, sicurezza, protezione dei dati personali, certificazioni e di quant'altro possa comunque interessare l'ambito della presente fornitura, compresi i successivi aggiornamenti.
Inoltre, gli Enti che potranno aderire alla Convenzione adottano al proprio interno policy, linee guida, disciplinari in ambito ICT e sicurezza informatica che il Fornitore è tenuta a rispettare.

9. LOTTI 1 - 2. QUALITA' E LIVELLI DEI SERVIZI

Il Fornitore dovrà produrre ed inviare all'Amministrazione, con cadenza trimestrale e in corrispondenza di ciascun trimestre di fatturazione e all'indirizzo di posta elettronica da essa indicato, un report con i dati relativi ai livelli di servizio, effettivamente conseguiti, per ciascuno dei tre mesi cui il report si riferisce, nell'ambito del contratto di fornitura. Tale report dovrà essere inviato entro i 20 giorni successivi alla chiusura del trimestre di riferimento al Referente tecnico dell'Amministrazione.

Il report dovrà contenere tutti i dati relativi ai livelli di servizio previsti nelle Tabelle dalla 1 alla 10 del successivo paragrafo per il lotto di riferimento. Dovranno essere pertanto forniti i dati analitici, estrapolati dai sistemi di trouble ticketing con dettaglio tale da consentire all'Amministrazione la verifica sia della correttezza dei dati relativi al singolo intervento, sia del calcolo degli SLA conseguiti in ciascun mese.

Ricordando che l'erogazione dei servizi della presente Convenzione avverrà, se non diversamente specificato in altre parti del Capitolato, per il Lotto 1 all'interno di 3 fasce orarie: orario Base, orario Esteso ed orario Continuato, per il Lotto 2 all'interno di 2 fasce orarie: orario Base e orario Continuato, i valori dei parametri di SLA saranno misurati, come dettagliato nelle successive tabelle, in riferimento alla finestra temporale di erogazione dei servizi precedentemente riportata.

9.1 SLA

Nel presente paragrafo sono elencati i Livelli di Servizio oggetto di monitoraggio. Per ciascuno dei Livelli di Servizio è definito uno SLA minimo, corrispondente alla qualità prevista dalla Convenzione.

I valori di SLA si applicano sui servizi dove il Fornitore ha il controllo completo della filiera tecnologica e non sui sistemi PaaS e SaaS di fornitori terzi di servizi in cloud.

Tutti gli SLA delle Tabelle 1, 8, 9 e 10 sono espressi in giorni lavorativi, mentre i tempi previsti nelle Tabelle 2, 3, 4, 5, 6 e 7 sono da riferirsi alle finestre di erogazione dei servizi definiti nel precedente paragrafo 5.1. In tali casi, quando lo SLA è espresso in giorni, è da intendersi entro l'n-esimo giorno lavorativo (all'interno cioè della finestra di erogazione) successivo a quello di apertura del ticket.

Gli SLA di cui alle Tabelle 2, 3, 4, 5, 6 e 7 sono tutti riferiti, anche ai fini del calcolo delle penali, ad un periodo di osservazione mensile e, nel caso in cui un'attività sia eseguita a cavallo di due periodi di osservazione, essa verrà riferita al periodo di osservazione in cui l'attività è completata.

Tabella 1 – SLA Assessment, Piano di Esecuzione e Avvio dei Servizi (Lotto 1 e Lotto 2)

Tipologia Servizio	Descrizione KPI	SLA Minimo – GG Lavorativi
Assessment e Piano Esecuzione dei Servizi	Tempo dall'invio della Richiesta di Assessment da parte dell'Amministrazione, alla conclusione delle attività di sopralluogo	entro **20 gg** (entro **30 gg** per un numero di sedi coinvolte maggiore di 3)
	Tempo dall'invio della Richiesta di Assessment da parte dell'Amministrazione, all' invio all'Amministrazione del Piano di Esecuzione dei Servizi	entro **40 gg** (entro **50 gg** per un numero di sedi coinvolte maggiore di 3)
	Tempo dall'invio delle richieste di modifica al Piano da parte dell'Amministrazione, all' invio all'Amministrazione del nuovo Piano di Esecuzione dei Servizi	entro **20 gg**
Avvio dei Servizi	Tempo dall'emissione dell'Ordinativo di Fornitura Principale, all'avvio dei servizi	entro **10 gg**
	Tempo dall'invio della Richiesta di aggiornamento del Piano di Esecuzione dei Servizi da parte dell'Amministrazione, all' invio all'Amministrazione della comunicazione di validità della	entro **7 gg**

Tipologia Servizio	Descrizione KPI	SLA Minimo – GG Lavorativi
	richiesta stessa	
Aggiornamento del Piano di Esecuzione dei Servizi	Tempo dall'invio della Richiesta di aggiornamento del Piano di Esecuzione dei Servizi da parte dell'Amministrazione, alla conclusione delle attività di sopralluogo	entro **15 gg** (entro **25 gg** per un numero di sedi coinvolte maggiore di 3)
	Tempo dall'invio della Richiesta di aggiornamento del Piano di Esecuzione dei Servizi da parte dell'Amministrazione, all' invio all'Amministrazione del Piano di Esecuzione dei Servizi aggiornato	entro **30 gg** (entro **40 gg** per un numero di sedi coinvolte maggiore di 3)
	Tempo dall'invio delle richieste di modifica al Piano da parte dell'Amministrazione, all' invio all'Amministrazione del nuovo Piano di Esecuzione dei Servizi Aggiornato	entro **10 gg**
Avvio dei nuovi Servizi	Tempo dall'emissione dell'Ordinativo di integrazione, all'avvio dei servizi	entro **10 gg**

Tabella 2 – SLA Gestione Sistemi, Rete (Lotto 1)

Tipologia Servizio	Descrizione KPI	Livello		
		Sistema Non Critico	Sistema Business Critical	Sistema Mission Critical
Presa in carico	Tempo di presa in carico malfunzionamento	Entro 4 ore	Entro 2 ore	Entro 1 ora
Risoluzione Malfunzionamento nella conduzione dei sistemi	Tempo di risoluzione malfunzionamento	Entro 8 ore	Entro 4 ore	Entro 2 ore
Intervento pianificato nell'ambito della conduzione dei sistemi	Tempo di completamento intervento	Entro 12 ore	Entro 6 ore	Entro 3 ore

Tabella 3 – SLA NOC (Lotto 1)

Tipologia Servizio	Descrizione KPI	Livello		
		Sistema Non Critico	Sistema Business Critical	Sistema Mission Critical
Presa in carico	Tempo di presa in carico malfunzionamento /segnalazione da sistema di monitoraggio	Entro 4 ore	Entro 2 ore	Entro 1 ora
Risoluzione malfunzionamento	Tempo di risoluzione malfunzionamento / segnalazione da sistema di monitoraggio	Entro 8 ore	Entro 4 ore	Entro 2 ore

Tabella 4 – SLA service desk sistemistico (Lotto 1)

Tipologia Servizio	Descrizione KPI	Livello		
		Richiesta su Sistema Non Critico	Richiesta su Sistema Business Critical	Richiesta su Sistema Mission Critical
Richieste al Service Desk sistemistico	Tempo di gestione richieste service desk	Entro 8 ore	Entro 3 ore	Entro 2 ore
	Tasso di risoluzione ticket al service desk (esclusi interventi che richiedono manutenzione HW, e soluzioni IaaS, PaaS, SaaS di fornitori terzi).	Almeno 50%	Almeno 60%	Almeno 70%

Tabella 5 – SLA Gestione Apparati e Sistemi di Sicurezza (Lotto 2)

Tipologia Servizio	Descrizione KPI	Livello di severità		
		BASSA	MEDIA	ALTA
Presa in carico	Tempo di presa in carico malfunzionamento	Entro 4 ore	Entro 2 ore	Entro 1 ora
Risoluzione Malfunzionamento nella conduzione dei sistemi	Tempo di risoluzione malfunzionamento	Entro 8 ore	Entro 4 ore	Entro 2 ore
Intervento pianificato nell'ambito della conduzione dei sistemi	Tempo di completamento intervento	Entro 12 ore	Entro 6 ore	Entro 3 ore

Tabella 6: SLA Monitoraggio in tempo reale eventi di sicurezza (SOC) (Lotto 2)

Tipologia Servizio	Descrizione KPI	Livello di severità		
		BASSA	MEDIA	ALTA
Presa in carico di un alert e prima analisi	Tempo di prima analisi evento di sicurezza/incidente da sistema di monitoraggio indicazione prime contromisure da applicare (identificazione, verifica, notifica)	Entro 2 ore	Entro 1 ora	Entro 30 minuti
Azioni da intraprendere	Indicazione procedure operative di contenimento, gestione dell'incidente, ingaggio del Incident Response Team. Indicazione contromisure da applicare e risoluzione reattiva di incidente di sicurezza	Entro 4 ore	Entro 2 ore	Entro 1 ora

Tabella 7 – SLA Incident Response (Lotto 2)

Tipologia Servizio	Descrizione KPI	Livello di severità		
		BASSA	MEDIA	ALTA
Presa in carico di un alert	Tempo di rilevazione e presa in carico di un alert di incidente di sicurezza (da sistema di monitoraggio e/o da segnalazione SOC)	Entro 12 ore	Entro 8 ore	Entro 4 ore
Convalida e risoluzione	Validazione e gestione dell'incidente, Indicazione contromisure da applicare e risoluzione reattiva e proattiva di incidente di sicurezza	Entro 4 ore	Entro 2 ore	Entro 1 ora

Per quanto attiene all'affidabilità e alla tempestività (Tabella 8) della messa a disposizione delle risorse si deve fare riferimento a:

- la variazione delle risorse (VRIS) nel tempo (per ciascuna fornitura), calcolata secondo la seguente formula, non deve essere superiore al 15% al semestre:

  VRIS = RSOS / RERO * 100

  dove

  RSOS = numero risorse sostituite

  RERO = numero risorse erogate a tempo pieno nel periodo di riferimento
- il tempo di sostituzione/aggiunta di risorse su richiesta del Referente tecnico dell'Amministrazione (RTMP) (durata contrattuale di ciascuna fornitura) calcolato secondo la seguente formula, non deve essere superiore a 10 giorni lavorativi:

  RTMP = Data disponibilità della risorsa – Data della richiesta

Il Fornitore dovrà garantire il passaggio di consegne, senza oneri per l'Amministrazione, nel caso di sostituzione dei tecnici nel corso della validità del contratto. La verifica delle competenze e delle capacità dei nuovi tecnici andrà svolta preventivamente, con trasmissione ai referenti dell'Amministrazione dei relativi curricula, e sul campo durante l'attività di affiancamento, al termine della quale i nuovi tecnici dovranno essere in grado di lavorare in assoluta autonomia. La presa in carico di tale know-how dovrà avvenire a titolo non oneroso per l'Amministrazione.

Tabella 8 – SLA messa a disposizione delle risorse professionali (Lotto 1 e Lotto 2)

Tipologia Servizio	Descrizione KPI	Livello
Messa a disposizione delle risorse	Variazione risorse nel tempo	< 15% a semestre
	Tempo sostituzione / aggiunta	< 10 giorni lavorativi

Tabella 9 – SLA Reportistica (Lotto 1)

Tipologia Servizio	Descrizione KPI	SLA min – GG Lavorativi
Report degli Asset e dei Servizi per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	entro **20 gg**
Report dei Livelli di Servizio conseguiti per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	entro **20 gg**

Tabella 10 – SLA Reportistica (Lotto 2)

Tipologia Servizio	Descrizione KPI	SLA min – GG Lavorativi
Report Servizi di sicurezza per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	entro **20 gg**
Report dei Livelli di Servizio conseguiti per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	entro **20 gg**

ALLEGATI

È parte integrante del presente Capitolato l'Allegato A – Figure professionali