



**APPALTO SPECIFICO PER LA FORNITURA DI SERVIZI DI IT SYSTEM MANAGEMENT  
INDETTO NELL'AMBITO DEL SISTEMA DINAMICO DI ACQUISIZIONE (SDA)**

**ALLEGATO 3 - CAPITOLATO TECNICO**

**CIG 7287025343**

## INDICE

1. PREMESSA.....	4
2. OGGETTO DELL'ACQUISIZIONE.....	4
3. CONTESTO TECNOLOGICO DELLA FORNITURA .....	4
4. CARATTERISTICHE, MODALITA' E SPECIFICHE DEI SERVIZI.....	7
4.1 Servizi di Monitoraggio Sistemi, Reti e sicurezza .....	7
4.2 Servizi di Conduzione Operativa Sistemi .....	13
4.2.1 Presa in carico di nuovi Servizi e Tecnologie.....	14
4.2.2 Gestione Piattaforme Elaborative .....	15
4.2.3 Gestione delle Procedure Batch .....	16
4.2.4 Gestione Alta Affidabilità.....	16
4.2.5 Gestione dello Storage .....	17
4.2.6 Backup e Restore Management.....	17
4.2.7 Gestione Database.....	18
4.2.8 Gestione Dominio .....	18
4.2.9 Gestione Middleware .....	19
4.2.10 Definizione delle Procedure Operative .....	20
4.2.11 Gestione Piattaforme di Posta Elettronica .....	20
4.3 Servizi di Conduzione Operativa Reti.....	21
4.4 Servizi di Sviluppo e Integrazione Architetture e Sistemi .....	23
4.5 Servizi di Rete: progettazione e sviluppo.....	26
4.6 Servizi di Sicurezza ICT: progettazione e sviluppo .....	27
4.7 Servizi di Service e Performance Management .....	30
4.7.1 Gestione delle Richieste e delle Segnalazioni.....	30
4.7.2 Supporto al Processo di Incident e Problem Management .....	31
4.7.3 Supporto al Processo di Change e Release & Deployment Management.....	32
4.7.4 Supporto al Processo di Service Asset & Configuration Management .....	32
4.7.5 4.7.5 Supporto al Processo Capacity Management.....	33
4.7.6 ServiceDesk Sistemistico .....	33
5. MODELLI DI EROGAZIONE E REMUNERAZIONE DEI SERVIZI.....	34
5.1 Servizi standard a Canone .....	35
5.1.1 Orari del servizio.....	36

5.1.2	Classificazione dei sistemi e livello di criticità.....	37
5.1.3	Reperibilità ed interventi fuori orario .....	37
5.2	Supporto Specialistico .....	38
5.2.1	Attività di supporto continuativo .....	39
5.2.2	Attività di supporto a richiesta .....	39
5.3	Modalità di attivazione ed esecuzione della fornitura.....	40
5.4	Documentazione.....	41
5.5	Orario e luogo di lavoro .....	41
5.6	Avvicendamento contrattuale.....	41
6.	CARATTERISTICHE DELLE FIGURE PROFESSIONALI .....	42
6.1	Figure professionali.....	42
7.	SERVIZIO DI ASSESSMENT E DI DEFINIZIONE DEL PIANO DI ESECUZIONE DEI SERVIZI .....	42
7.1	Assessment .....	42
7.2	Piano di Esecuzione dei Servizi .....	43
8.	OSSERVANZA DI NORME, LEGGI E REGOLAMENTI .....	46
9.	QUALITA' E LIVELLI DEI SERVIZI.....	46
9.1	SLA .....	46

## **1. PREMESSA**

Il presente Capitolato Tecnico disciplina gli aspetti tecnici della Convenzione relativa alla fornitura di servizi di IT System Management per le Pubbliche Amministrazioni della Regione Emilia-Romagna.

## **2. OGGETTO DELL'ACQUISIZIONE**

L'oggetto della fornitura 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, ovvero il complesso dei servizi e delle attività volti 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 e l'integrità dei relativi dati nonché a fornire il supporto necessario per garantirne il costante allineamento con l'evoluzione tecnologica del mercato ICT 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.

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 ICT e ampiamente utilizzate dalle Pubbliche Amministrazioni. Di seguito viene fornita, a titolo puramente indicativo e non esaustivo, una panoramica degli ambiti tecnologici in questione.

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 e/o CED 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).

Ciascuna Amministrazione può disporre di apparecchiature hardware e prodotti software di base di varia tipologia e 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 si impegna ad erogare i servizi di system management 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	Unix (AIX, HP-UX, Solaris), Linux (Red Hat, CentOS, Ubuntu, FreeBSD, Debian, Suse), 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)
data management and integration	database management systems and tools (administration, utilities, monitoring) (DB2, Oracle, SQL Server, MySQL, PostgreSQL)
	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)
	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)
security software	data security (encryption), endpoint security (antivirus), identity and access management (single sign-on), network security (firewall, VPN)
<b>Enterprise Software</b>	
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 BPC, SAP HR ed eRecruiting, Oracle JD Edwards EnterpriseOne, SAGE ERP X3
<b>Software Client</b>	
Client software	sistemi operativi client e dispositivi mobili (Windows, Apple, Android)
	prodotti software di informatica individuale (MS Office, MS SharePoint, OpenOffice)
	web browser (Internet Explorer, Firefox, Chrome, Safari)
	antivirus (MCAfee, Norton, Kaspersky)
	Sistemi di virtualizzazione (XenApp, XenDesktop)
	software distribution e remote desktop control
<b>Tecnologie Hardware</b>	
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)
<b>Tecnologie Cloud</b>	
	Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform

Public Cloud	(GCP)

#### 4. CARATTERISTICHE, MODALITA' E SPECIFICHE DEI SERVIZI

Di seguito sono descritti in dettaglio i servizi richiesti oggetto della Convenzione.

##### 4.1 SERVIZI DI MONITORAGGIO SISTEMI, RETI E SICUREZZA

Il “**Servizio di Monitoraggio Sistemi, Reti e Sicurezza**” annovera al suo interno sia i servizi di monitoraggio operati sullo strato network dell’architettura (sotto servizio erogato dal **NOC – Network Operation Center**) sia i servizi di monitoraggio relativi agli aspetti legati alla sicurezza dell’architettura (sotto servizio erogato dal **SOC – Security Operation Center**).

In particolare, il sotto servizio **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. Per quanto attiene il sotto servizio **SOC**, le funzioni previste affiancano l’attività di monitoraggio del **NOC**, e prevedono il monitoraggio di tentativi di intrusione o di attacco oltre che eventuali falle di sicurezza. Sarà altresì compito del **SOC** la rilevazione dei livelli di sicurezza (antivirus e allineamento delle configurazioni alle policy di sicurezza dei sistemi dell’Amministrazione).

Pertanto, il Fornitore deve disporre all’interno del proprio Centro Servizi per l’Operatività da Remoto sia del servizio **NOC** che del servizio **SOC**, 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 alla Ditta aggiudicataria 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, la ditta aggiudicataria deve adeguatamente formare ed istruire il personale del NOC, relativamente all'infrastruttura ICT dell'Amministrazione stessa.

Il NOC della ditta aggiudicataria 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 ed, in nessun caso, potrà essere utilizzata, anche parzialmente, la banda trasmissiva a disposizione dell'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 team impegnati nell'erogazione dei servizi:
  - 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) l'autenticazione e la profilazione delle utenze al punto di accesso alla rete dell'Amministrazione;

- c) la tracciatura degli accessi ai sistemi (es. 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) 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 Incident 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

	<p>modalità note come “Stateful inspection”.</p> <p>Devono essere utilizzati sistemi/meccanismi di intrusion detection e prevention che analizzino il traffico in entrata ed in uscita dalla rete dell’Amministrazione.</p>
Riservatezza dei dati e delle trasmissioni	Deve essere garantita la riservatezza di tutti i dati gestiti.
Integrità dei dati	<p>Devono essere adottati antivirus centralizzati ad aggiornamento periodico, che analizzino e bonifichino gli eventuali codici malevoli.</p> <p>Devono essere adottati antivirus su tutte le postazioni utilizzate dal personale del Fornitore e collegate con la rete dell’Amministrazione.</p> <p>Tali postazioni devono soddisfare lo standard per le postazioni di lavoro Previste per l’Amministrazione</p>
Auditing e vulnerabilità assessment	<p>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.</p>
Amministrazione accessi	<p>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.</p>

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.

## SERVIZIO DI MONITORAGGIO

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 dalla Ditta aggiudicataria (se richiesto dall'Amministrazione) dovrà essere installato su server di proprietà dell'Amministrazione stessa.

Compito della Ditta aggiudicataria sarà in particolare:

- 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 sviluppato “ad hoc”, verifica di URL, query sui principali DB (Oracle, MySQL, SQLServer), 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.

#### 4.2 SERVIZI DI CONDUZIONE OPERATIVA SISTEMI

La “**Conduzione Operativa Sistemi**” comprende sia i servizi base di gestione continuativa (sotto servizio “**Server logici e fisici**”) sia i servizi di gestione delle piattaforme di memorizzazione e archiviazione (sotto servizio “**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 sotto servizio 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 macro categoria “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 schedate;
- 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.

#### *4.2.1 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.

#### 4.2.2 *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, Mainframe, 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, ecc.);
- 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.

#### 4.2.3 *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 ambito mainframe e ambienti open.

#### 4.2.4 *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 ecc.), 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.

#### 4.2.5 *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.

#### 4.2.6 *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.

#### 4.2.7 *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.

#### 4.2.8 *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/WINS

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.

#### 4.2.9 *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, ecc.) utilizzando gli strumenti propri di ogni singolo middleware (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.

#### *4.2.10 Definizione delle Procedure Operative*

E' 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 effettuare 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.

#### *4.2.11 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 mantenere 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.

### **4.3 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.

#### **4.4 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 puo' comprendere Mainframe, 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 mantenere 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.).

#### 4.5 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 e eliminazione delle obsolescenze eventualmente in essere.

In particolare il servizio in oggetto:

- Effettua le attività di assessment degli apparati e della qualità della comunicazione fra gli stessi;
- Effettua la migrazione degli apparati obsoleti verso nuove architetture;
- 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 necessità aziendali di trasferimento dati, individuando i diversi tipi di trasferimento: video e voce unidirezionali, sia di tipo unicast che di tipo broadcast, video e voce bidirezionali, incluse le teleconferenze;
- Supporta l’identificazione delle possibilità di comunicazioni non cablate (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 ICT 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;

#### **4.6 SERVIZI DI SICUREZZA ICT: PROGETTAZIONE E SVILUPPO**

I “**Servizi di Sicurezza ICT, Progettazione e Sviluppo**” costituiscono di fatto il ruolo operativo del SOC. Il servizio è 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 effettuata all'interno di questo servizio anche la 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 (penetration test).

Il servizio di sicurezza ICT progetta e realizza le contromisure di tipo tecnologico volte alla difesa perimetrale e di contenuto del sistema informativo. Tale servizio ha lo scopo di:

- attuare la politica per la sicurezza ai flussi di rete in termini di tipo e/o contenuto del traffico;
- monitorare e verificare l'efficacia delle misure di sicurezza adottate per i flussi di rete;
- 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;
- fornire supporto all'Amministrazione nell'adeguamento delle politiche e delle misure di sicurezza con particolare riferimento a quanto previsto dal GDPR (Regulation (EU) 2016/679)

Il Fornitore è responsabile:

- della gestione degli elementi di sicurezza presenti presso l'Amministrazione secondo quanto descritto nel presente capitolato tecnico, ovvero di quanto concordato con l'Amministrazione stessa sulla base delle procedure e delle politiche definite;
- dell'attuazione di contromisure finalizzate al mantenimento dei livelli di sicurezza stabiliti;
- della risoluzione reattiva o proattiva di incidenti di sicurezza;
- del controllo del traffico di rete;
- della gestione, verifica, analisi, correlazione e storicizzazione degli allarmi generati e delle informazioni raccolte nei file di log delle infrastrutture di sicurezza e di rete;
- della produzione periodica dei Report di Sicurezza con i dati collegati alle attività di gestione della sicurezza logica;
- delle attività di updating e upgrading delle versioni dei prodotti di sicurezza;
- del backup dei log e delle configurazioni.

All'attivazione del contratto saranno definiti e formalizzati i processi da applicare alla gestione 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).

Dal punto di vista operativo, il Fornitore supporta l'Amministrazione nell'erogazione di uno o più dei seguenti servizi:

- 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, ecc.)

- Servizio di gestione IDS (Intrusion Detection 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 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; 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 security host hardening; Il servizio provvede alla definizione, manutenzione e controllo delle politiche di configurazione e di aggiornamento dei sistemi server e storage.

Nel caso di variazioni delle Politiche di Sicurezza, i nuovi requisiti o le modifiche dei requisiti esistenti saranno implementati mediante un processo specifico che prevede la progettazione, 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.

E' richiesto inoltre che, sotto la supervisione dell'Amministrazione, il Fornitore debba prestare supporto all'Amministrazione per l'esecuzione dei test di vulnerabilità che 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 implementare le azioni correttive per la rimozione di eventuali criticità individuate.

Tuttavia, considerando la responsabilità generale del Fornitore di mantenere i sistemi in perfetta efficienza, risulta evidente che le attività di rilevazione e di bonifica delle vulnerabilità potranno essere svolte anche in modo autonomo, indipendentemente dall'attività dell'Audit IT.

#### **4.7 SERVIZI DI SERVICE E PERFORMANCE MANAGEMENT**

E' 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.

##### *4.7.1 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.

#### 4.7.2 *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.

E' 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.

#### *4.7.3 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.

#### *4.7.4 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.

#### 4.7.5 4.7.5 *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.

#### 4.7.6 *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);
- assegnamento 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;
- assegnamento 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.

## **5. MODELLI DI EROGAZIONE E REMUNERAZIONE DEI SERVIZI**

Nei capitoli precedenti i servizi di System Management 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 macro-categorie 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 e le relative modalità di remunerazione sono sintetizzate nella tabella seguente:

Macro Categoria	Modalità di remunerazione
Sistemi e Apparati di rete; Sistemi mail server; Sistemi DB server; Sistemi Web server; Sistemi Back office; Sistemi Storage backup; Sistemi di protezione e altri apparati di rete.	Canone
<b>Figure Professionali:</b> TEM - ICT Operation Manager; CET - Enterprise Architect; SPP - System Architect; SIS - System Administrator; SIJ - System Administrator Junior; DBS - Database Administrator Senior; DBJ - Database Administrator Junior; ESI - ICT Security Specialist - Analista di processo per la sicurezza delle informazioni; SAS - ICT Security Specialist - Specialista di processo della sicurezza delle informazioni; SAJ - ICT Security Specialist - Specialista infrastrutturale della sicurezza delle informazioni; SRS - Network Specialist Senior; SRJ - Network Specialist Junior.	GG/uomo

## 5.1 SERVIZI STANDARD A CANONE

Nell'ambito della presente Convenzione sono definite due distinte modalità di presidio del servizio:

**-Presidio on-site:** i servizi sono erogati da personale del Fornitore allocato fisicamente nella sede dell'Amministrazione, quindi con risorse dedicate. Sarà cura dell'Amministrazione mettere a disposizione del fornitore degli strumenti ed i software necessari all'erogazione del servizio.

**-Presidio remoto:** i servizi sono erogati mediante connessione telematica da personale del Fornitore allocato nella propria sede. Nel costo del servizio è inclusa, in particolare, la messa a disposizione del Centro Servizi stesso e degli strumenti in esso presenti e dei software necessari all'erogazione

del servizio. Laddove per specifiche esigenze dell'Amministrazione fosse richiesto l'utilizzo di software diverso da quello nelle disponibilità del Centro Servizi del Fornitore, l'eventuale extra costo in termini di licenze sarà valutato a parte, in fase di assessment, e comunque a carico dell'Amministrazione.

Il “**Servizio di monitoraggio sistemi, reti e sicurezza**” 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 schedate.

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**” e “**conduzione operativa reti**” comprende in generale tutti i **servizi base di gestione** di tipo continuativo svolti nell'orario base di lavoro, includendo gestione sistemi e reti, manutenzione sistemi, gestione software di base e di ambiente e basi dati, gestione sicurezza logica, gestione configurazione.

I servizi di “**Monitoraggio sistemi, reti e 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.

Per entrambi i servizi la **remunerazione del servizio è a canone** ed è basata sulla dimensione 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 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.

### 5.1.1 Orari del servizio

L'effort dedicato alle attività di monitoraggio sistemi, conduzione operativa dei sistemi e delle reti 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, tre fasce orarie di riferimento:

<b>Finestra di erogazione dei servizi</b>		
<b>Orario BASE</b>	<b>Orario ESTESO</b>	<b>Orario CONTINUATO</b>
Lun-Ven 8.00 – 17.00	Lun-Ven 8.00 – 18.00;	H24, 7 giorni su 7

	Sab 8.00 - 14.00	
--	------------------	--

### 5.1.2 Classificazione dei sistemi e livello di criticità

I server logici possono essere classificati in base al livello di complessità e criticità; nel contesto della presente Convenzione si definiscono **quattro classi di complessità e tre classi di criticità**:

- Classificazione per livello di complessità

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

- Classificazione per livello di criticità

- **Server non critico**: disponibilità  $\leq 99,8\%$ , tempo di presa in carico malfunzionamenti entro 4 ore, ambiente non di produzione (*Tipicamente sistemi di test/sviluppo o sistemi che comunque non impattano in modo significativo sui processi di business dell'Ente*);
- **Server Business critical**: disponibilità  $> 99,8\%$ , tempo di presa in carico malfunzionamenti entro 2 ore, ambiente di produzione (*Tipicamente sistemi di produzione che impattano in modo significativo sui processi di business dell'Ente*);
- **Server Mission critical**: disponibilità  $> 99,8\%$ , tempo di presa in carico malfunzionamenti entro 1 ora, ambiente di produzione (*Tipicamente sistemi di produzione il cui malfunzionamento blocca i processi di business dell'Ente*).

I criteri di classificazione per livello di complessità, che associano sia i server logici che fisici alle classi suddette, sono criteri che concorrono alla formazione del canone base annuo (e sono definiti dall'Amministrazione nella fase di assessment iniziale, vedasi paragrafo 7.1):

### 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, 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 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 i 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.

### 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.

Nella tabella seguente sono sintetizzati i possibili elementi di costo per il servizio di supporto specialistico a richiesta: ciascun elemento rappresenta la tariffa giornaliera per il supporto specialistico a richiesta di una specifica figura professionale.

<b>TEM: ICT Operation Manager</b>
<b>CET: Enterprise Architect</b>
<b>SPP: System Architect</b>
<b>SSS: System Administrator Senior</b>
<b>SIS: System Administrator</b>
<b>SIJ: System Administrator Junior</b>
<b>DBS: Database Administrator Senior</b>
<b>DBJ: Database Administrator Junior</b>
<b>ESI: ICT Security Specialist - Analista di processo per la sicurezza delle informazioni</b>
<b>SAS: ICT Security Specialist - Specialista di processo della sicurezza delle informazioni</b>
<b>SAJ: ICT Security Specialist - Specialista infrastrutturale della sicurezza delle informazioni</b>
<b>SRS: Network Specialist Senior</b>
<b>SRJ: Network Specialist Junior</b>

### **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 dalla Ditta aggiudicataria; l'Amministrazione si riserva la facoltà di ricusare detto personale per giustificati motivi.

E' 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 nella presente Convenzione 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 e saranno oggetto di valutazione. 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. 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. CARATTERISTICHE DELLE FIGURE PROFESSIONALI**

### **6.1 FIGURE PROFESSIONALI**

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

## **7. 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 individua le caratteristiche:

- delle apparecchiature da gestire/manutenere e, per ciascuna di esse, 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 mantenere;
- 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.

Per quanto riguarda più in dettaglio le attività, esse potranno essere acquisite 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, relative ai soli apparati per i quali l'Amministrazione richieda il servizio di manutenzione HW, 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, e per i quali il Fornitore si avvarrà della facoltà di non prestare il servizio di manutenzione;
- 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;
- determinare il "valore di manutenzione" dell'apparato.

## **7.2 PIANO DI ESECUZIONE DEI SERVIZI**

Il Piano di Esecuzione dei Servizi dovrà contenere:

### **Risultati dell'Assessment**

- Elenco sintetico, e completo in allegato, 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 od 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:
  - o 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;
  - o descrizione delle attività che saranno svolte con indicazione della frequenza programmata;
- Definizione dei processi che regoleranno l’esecuzione dei servizi, relativamente alle attività:
  - o di ordinaria gestione/manutenzione (ad esempio: monitoraggio apparati, interventi di manutenzione preventiva, etc.);
  - o eseguite a seguito di specifiche richieste dell’Amministrazione;
  - o scaturite da richieste di assistenza o segnalazione di malfunzionamenti, con descrizione dell’iter di escalation;
  - o di change management, con riferimento alle politiche ed ai processi di change, e alle procedure di ripristino;
  - o di terze parti (ad esempio: 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:
  - o presa in carico degli apparati e start up dei servizi, con indicazione di quali saranno svolte in loco;
  - o configurazione apparati e/o installazione software per la gestione da remoto;
  - o 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, e 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 servizi a consumo (GG/uomo). Tale importo forfettario è destinato alla copertura finanziaria dei servizi che verranno via via fatturati in base ai consumi e, anche se indicato in maniera presuntiva, concorre nella sua interezza al computo del valore dell'Ordinativo di Fornitura Principale o collegato, ai fini dell'erosione del massimale. Si precisa comunque che detti importi forfettari non sono vincolanti 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 con le procedure previste.

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. OSSERVANZA DI NORME, LEGGI E REGOLAMENTI**

La Ditta aggiudicataria è tenuta all'osservanza delle norme di legge e di regolamento adottate dalle Autorità competenti in materia di contratti di lavoro, sicurezza, protezione dei dati personali e di quant'altro possa comunque interessare la presente procedura, e successivi aggiornamenti.

Inoltre, gli Enti che potranno aderire alla Convenzione adottano al proprio interno policy, linee guida, disciplinari in ambito ICT e sicurezza IT che la Ditta aggiudicataria è tenuta a rispettare.

## **9. 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 nella Tabella 1, Tabella 2, Tabella 3, Tabella 4, Tabella 5 e Tabella 6 del successivo paragrafo. Dovranno essere pertanto forniti i dati analitici, estrapolati dal sistema 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, all'interno di 3 fasce orarie: orario Base, orario Esteso ed orario Continuato, come dettagliato nella successiva tabella, I valori dei parametri di SLA saranno misurati 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 di tali Livelli di Servizio è definito uno SLA minimo, corrispondente alla qualità prevista dalla Convenzione.

Tutti gli SLA della Tabella 1 e della Tabella 6 sono espressi in giorni lavorativi, mentre i tempi previsti nella Tabella 2, Tabella 3, Tabella 4 sono da riferirsi agli orari di erogazione dei servizi definiti nel precedente paragrafo. 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 alla Tabella 2, Tabella 3 e Tabella 4 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

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 <b>20 gg</b> (entro <b>30 gg</b> 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 <b>40 gg</b> (entro <b>50 gg</b> 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 <b>20 gg</b>
Avvio dei Servizi	Tempo dall'emissione dell'Ordinativo di Fornitura Principale, all'avvio dei servizi	entro <b>10 gg</b>
Aggiornamento del Piano di Esecuzione	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 richiesta stessa	entro <b>7 gg</b>
	Tempo dall'invio della Richiesta	entro <b>15 gg</b> (entro <b>25 gg</b> per un

dei Servizi	di aggiornamento del Piano di Esecuzione dei Servizi da parte dell'Amministrazione, alla conclusione delle attività di sopralluogo	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 <b>30 gg</b> (entro <b>40 gg</b> 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 <b>10 gg</b>
Avvio dei nuovi Servizi	Tempo dall'emissione dell'Ordinativo di integrazione, all'avvio dei servizi	entro <b>10 gg</b>

Tabella 2 – SLA Gestione Server, Rete, Sicurezza

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 / SOC

Tipologia Servizio	Descrizione KPI	Livello		
		Sistema Non	Sistema Business	Sistema Mission



		Critico	Critical	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

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)	Almeno 50%	Almeno 60%	Almeno 70%

#### **Affidabilità e tempestività della messa a disposizione delle risorse**

Relativamente al gruppo di lavoro richiesto dall'Amministrazione, si applicano i seguenti indicatori: Nell'ambito di ciascuna fornitura la variazione delle risorse (VRIS) nel tempo, 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

Nell'ambito della durata contrattuale di ciascuna fornitura, il tempo di sostituzione/aggiunta di risorse su richiesta del Referente tecnico dell'Amministrazione (RTMP) calcolato secondo la seguente formula, non deve essere superiore a 10 giorni lavorativi:

$$RTMP = \text{Data disponibilità della risorsa} - \text{Data della richiesta}$$

Tabella 5 – SLA messa a disposizione delle risorse professionali

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

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 6 – SLA Reportistica

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 <b>20 gg</b>
Report dei Livelli di Servizio conseguiti per l'Amministrazione	Tempo dalla chiusura del trimestre di riferimento, all'invio del report all'Amministrazione	entro <b>20 gg</b>

## **ALLEGATI**

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