**MINISTERO DELL'INTERNO**

MINISTERO
DELL'INTERNO

# CAPITOLATO TECNICO

## Network Management e Trouble Ticket System

*Fornitura di un sistema informativo*

*per la gestione della rete e per la gestione dei ticket.*

# Sommario

## Indice delle Tabelle

# 1 PREMESSA

Il presente capitolato definisce gli aspetti tecnici della fornitura di un sistema informativo centralizzato di gestione della rete e della gestione dei ticket.
La fornitura prevede l'acquisizione di due sistemi informatici integrati (comprensivi dell'infrastruttura hardware e del software di base e applicativo) e dei relativi servizi di installazione, configurazione, assistenza e supporto specialistico. Inoltre dovrà essere erogato un periodo di formazione del personale dell'Amministrazione per poter mettere in condizioni gli amministratori del sistema e gli operatori di essere autonomi nella gestione quotidiana dell'infrastruttura e nell'apertura delle segnalazioni.

## 1.1 Sigle e acronimi

Nell'ambito del presente Capitolato Tecnico sono stati usati i seguenti acronimi:

Tabella 1 - Sigle e acronimi

| ACRONIMO | DESCRIZIONE |
|---|---|
| **CDP** | Cisco Discovery Protocol |
| **CSV** | Comma Separated Value |
| **DEC** | Direttore dell'Esecuzione del Contratto |
| **FSF** | Free Software Foundation |
| **GPL** | General Public License |
| **ICMP** | Internet Control Message Protocol |
| **LDAP** | Lightweight Directory Access Protocol |
| **LDS** | Livelli di Servizio |
| **LLDP** | Link Layer Discovery Protocol |
| **MIB** | Management Information Base |
| **ODL** | Ordini di Lavoro |
| **OSI** | Open Source Initiative |
| **RADIUS** | Remote Authentication Dial-In User Service |
| **RTI** | Raggruppamento Temporaneo d'Impresa |
| **SISIN** | Sistema di Supervisione Integrato |
| **SNMP** | Simple Network Management Protocol |
| **TTS** | Trouble Ticket System |

## 1.2 Definizioni

Nel corpo del presente documento i termini e le espressioni di seguito indicati devono essere interpretati secondo le seguenti definizioni:

- Fornitore: la società aggiudicataria della gara, eventualmente mandataria di un RTI;
- Sistema informativo: l'insieme delle apparecchiature, delle applicazioni e dei servizi che permettono all'Amministrazione di poter raccogliere, elaborare, memorizzare i dati al fine di supportare il processo di gestione della rete Dipartimentale;
- Sistema informatico: l'insieme dell'infrastruttura hardware e del software di base e applicativo;

- Assistenza: l'insieme delle operazioni volte a mantenere in efficienza e/o ripristinare la piena funzionalità dei sistemi richiesti nel Capitolato Tecnico;
- Guasto bloccante: Si intende per guasto bloccante un malfunzionamento per cui è impedito l'uso di tutto il sistema o di una o più funzioni essenziali.
- Guasto non bloccante: Si intende per guasto non bloccante un malfunzionamento per cui è impedito l'uso di funzionalità non essenziali o critiche del sistema in alcune condizioni per cui non si ha un effetto penalizzante sull'operatività degli utenti.
- Incidente: evento che non è parte delle operazioni standard di un servizio, e che causa, o potrebbe causare, un'interruzione o una riduzione della qualità del servizio stesso.
- Malfunzionamento: è un impedimento all'esecuzione dell'applicazione /funzione o gli effetti che un errore ha causato sulla base dati o il riscontro di differenze fra l'effettivo funzionamento del software applicativo e quello atteso, come previsto dalla relativa documentazione.

# 2 SITUAZIONE ATTUALE

L'Amministrazione utilizza, attualmente, un sistema informatico di monitoraggio della rete, operativo dal 2009, denominato *Sistema di Supervisione Integrato* (Si.S.In.) realizzato dalla società *Telecom Italia S.p.A.* sulla base delle esigenze, al tempo, manifestate. Il Si.S.In è composto da software di mercato e da moduli software sviluppati ad hoc e brevettati che garantiscono una esperienza utente unificata su tutte le componenti.
Il Si.S.In. consente agli operatori, tramite una console unica, di visualizzare in modo omogeneo gli eventi rilevati sugli apparati sottoposti a monitoraggio sfruttando i protocolli ICMP e SNMP, indipendentemente dalla particolarità della piattaforma che li genera. La soluzione permette di supervisionare in modo efficace e proattivo gli apparati gestiti.
Gli eventi di allarme sono visualizzati sia in modalità testuale che in forma grafica geolocalizzata.
Sulle mappe sono evidenziate le sedi dove sono ubicati gli apparati, con degli indicatori cromatici che si aggiornano in base allo stato operativo degli apparati stessi. Le variazioni di stato sono evidenziate con differenti tonalità di colore (es. etichetta verde: apparato funzionante, etichetta rossa: apparato guasto o non raggiungibile).
Le informazioni attinenti ad ogni apparato gestito e le relazioni tra le caratteristiche tecniche degli stessi, congiuntamente alle relative informazioni di tipo logistico e amministrativo, sono conservati all'interno di un'apposita base dati relazionale.
Il Si.S.In. dispone, inoltre, di una funzionalità di Data Collection, attraverso la quale avviene la ricezione degli indicatori di qualità dai sistemi alimentanti (Performance Management, Service Assurance).
Attraverso la manipolazione, l'integrazione, la correlazione dei dati raccolti, in modo automatico il Si.S.In. realizza, quindi, le funzionalità legate alla gestione della reportistica relativa al monitoraggio delle performance dei servizi di assistenza tecnica e manutenzione delle infrastrutture di trasporto dati geografiche. L'analisi della reportistica dà una visione di sintesi della qualità del servizio erogato agli utenti, nonché evidenzia l'eventuale mancato rispetto dei termini contrattuali da parte delle società per l'applicazione delle penali.
Il portale di accesso rappresenta il punto di accesso unico agli strumenti e alle funzionalità della piattaforma Si.S.In..
Il Si.S.In. comprende:

- strumenti di supporto alla Web Collaboration e di Knowledge Management;
- accesso al TTM, al Self Ticketing e al TTM ODL;
- accesso ai report e ai dati presenti nel data base;
- link al sistema di supervisione, storico degli allarmi di rete, performance e gestione degli SLA, gestione delle configurazioni;

- link agli Element Manager;
- accessi Profilati: gestione delle profilature utenti con creazione di viste personalizzate in base al ruolo ricoperto all'interno dell'organizzazione;
- sicurezza dei dati: il sistema è dotato di meccanismi di protezione dei dati attraverso gestione dei profili di accesso delle utenze autorizzate e crittografia della sessione;
- protezione dei dati;
- procedure automatiche e regolari di back-up per il salvataggio di tutte le informazioni.

Oltre al monitoraggio degli allarmi, il Si.S.In., mette a disposizione un limitato insieme di funzionalità per il controllo delle centrali telefoniche e dal traffico da esse generato, derivante dalla piattaforma separata di gestione delle stesse.

## 2.1 Dimensionamento

Di seguito si riportano le consistenze dell'attuale sistema di gestione.

- Apparati posti sotto monitoraggio: 6500.
- Numero di utenti censiti: 250.
- Numero di utenti concorrenti: 30.
- Numero di ticket annui: 6000.

Inoltre si riportano, a titolo esemplificativo ma non esaustivo, i produttori degli apparati monitorati dal Si.S.In., si precisa che tutti gli apparati rispondono al protocollo SNMP:

- Airfiber;
- Allied Telesis;
- Amtec;
- Brocade;
- Capetti;
- Cisco System;
- D-Link;
- Ericsson;
- Fortinet;
- Garrettcom;
- Huawei;
- Juniper Networks;
- Motorola;
- Palo Alto Networks;
- Radware;
- Tiesse;
- Townet;
- ZTE.

# 3 OGGETTO DELLA FORNITURA

L'oggetto della fornitura, descritto nel presente capitolato, consiste nel sistema informativo nel suo complesso rappresentato da hardware, software di base e software applicativo e dalle relative attività e servizi elencati nel seguito:

- fornitura di un sistema informatico per la gestione della rete;
- fornitura di un sistema informatico per la gestione dei ticket;
- attività di installazione e configurazione:
- servizio di assistenza e manutenzione evolutiva;
- supporto specialistico;
- formazione.

La fornitura dovrà conformarsi ai requisiti di base di seguito indicati:

- tutti i componenti dovranno soddisfare i requisiti e presentare caratteristiche tecniche non inferiori a quanto riportato nel presente capitolato tecnico;
- i componenti, laddove di pertinenza, dovranno essere forniti secondo le quantità, indicate nel presente capitolato tecnico;
- l'infrastruttura nel suo complesso ed i servizi ad essa correlati dovranno rispettare le normative vigenti in materia di sicurezza dell'informazione, di privacy, emissioni elettromagnetiche e sicurezza sul lavoro specificati nel paragrafo 3.4.

## 3.1 Sedi

Le attività saranno svolte presso il Compendio Viminale (Piazza del Viminale 1, Roma) secondo le modalità indicate nel presente documento.

## 3.2 Durata

I servizi oggetto della fornitura avranno una durata di 36 (trentasei) mesi.

## 3.3 Gestione della fornitura

Il fornitore dovrà individuare un Responsabile della Fornitura, che costituirà il singolo punto di contatto nei confronti dell'Amministrazione. Il Responsabile della Fornitura dovrà coordinare tutte le attività e produrre resoconti periodici, che saranno presentati durante i SAL di progetto.

- per ciascun prodotto il fornitore fornirà copia digitale e cartacea della manualistica tecnica completa;
- la documentazione dovrà essere in lingua italiana, oppure, se non prevista, in lingua inglese;
- per ciascun prodotto, il fornitore fornirà le licenze di utilizzo ed i supporti originali per l'installazione di tutto il software oggetto della fornitura, compresa la documentazione necessaria per un eventuale ripristino del sistema informatico.
- il fornitore dovrà garantire l'interoperabilità e la compatibilità di tutti i sistemi che costituiscono la soluzione proposta e l'integrazione con l'ambiente esistente.

## 3.4 Certificazioni e conformità

Tutto il materiale, pezzi o componenti non esplicitamente indicati nel presente capitolato, ma necessari per integrare le apparecchiature fornite con l'infrastruttura esistente, dovranno essere forniti senza ulteriori oneri. Sarà pertanto cura del fornitore evidenziare e inserire in offerta eventuali componenti aggiuntivi, ritenuti essenziali per il corretto montaggio e funzionamento dei sistemi, anche laddove questi non siano stati esplicitamente citati nel presente documento.
Tutte le apparecchiature e le opzioni eventualmente fornite dovranno essere nuove di fabbrica ovvero essere costruite utilizzando parti nuove.
Le apparecchiature offerte dovranno possedere marchi di certificazione riconosciuti da tutti i Paesi dell'Unione Europea, essere conformi alle norme concernenti la compatibilità elettromagnetica, alle normative CEI e, in generale, alla vigente normativa che disciplina i componenti e le relative modalità di impiego delle apparecchiature medesime ai fini della sicurezza degli utilizzatori. A titolo esemplificativo e non esaustivo, le apparecchiature fornite dovranno rispettare i requisiti indicati nella Direttiva CEE 90/270 recepita dalla legislazione italiana con Legge 19 febbraio 1992, n. 142 e quelli relativi:

- alla riduzione dell'uso di sostanze pericolose previsto dalla normativa vigente, ed in particolare dalla direttiva 2002/95/CE, (RoHS), recepita con D .Lgs. 151/2005;
- ai requisiti di immunità definiti dalla EN55024;

- alla conformità alle Direttive di Compatibilità Elettromagnetica (89/336 e 92/31 - EMC) e conseguentemente essere marchiate e certificate CE;
- ai requisiti di sicurezza (es.: IMQ) e di emissione elettromagnetica (es.: FCC classe A) certificati da Enti riconosciuti a livello europeo.

# 4 SISTEMA INFORMATICO PER LA GESTIONE DELLA RETE

Nel presente capitolo sono riportati i requisiti minimi che dovranno obbligatoriamente essere rispettati e supportati nella soluzione proposta dal fornitore per la gestione della rete.
La soluzione dovrà essere del tipo "tutto incluso" e quindi completa di hardware, software di base e software applicativo.
L'hardware dovrà essere dimensionato in modo da garantire le esigenze espresse dall'Amministrazione e riportate nel paragrafo 2.1 e, analogamente, il software dovrà essere opportunamente corredato di licenze d'uso in modo da garantire il monitoraggio di tutti gli apparati per i quali l'Amministrazione richiede tale servizio.
In particolare il software applicativo, di tipo *Web-based*, e il sistema operativo dovranno essere basati su soluzioni open source e il fornitore dovrà rilasciare all'Amministrazione, tutto il codice sorgente delle parti software sviluppate ad hoc per l'integrazione delle diverse soluzioni, opportunamente commentato e documentato.
Per soluzioni open source si intendono tutte le soluzioni che hanno licenze approvate esplicitamente dalla OSI oppure considerate dalla FSF libere (free) o compatibili con la GPL.
Per le sue caratteristiche e le funzioni cui sarà preposto, il sistema dovrà inoltre consentire lo scambio di informazioni con il sistema di gestione dei ticket.

## 4.1 Hardware

La fornitura dovrà prevedere una coppia di sistemi hardware ridondati e configurati in alta affidabilità sui quali installare il software di base e applicativo in modo da garantire continuità a quest'ultimo in caso di guasto di un singolo apparato o di un aggiornamento dell'architettura stessa.
Tutte le caratteristiche descritte nel presente paragrafo sono da intendersi come minime ed essere presenti su ognuno dei sistemi proposti:

- apparato da rack;
- doppia alimentazione;
- sistemi di ventilazione adeguati alla potenza dissipata e ridondati;
- interfacce di rete 2x1Gbps e 1x10Gbps;
- storage in raid 1 (mirroring).

Il fornitore dovrà garantire e certificare la compatibilità tra la soluzione hardware e le soluzioni software adottate.

## 4.2 Funzionalità

Nei sottoparagrafi seguenti vengono descritte tutte le funzionalità di gestione, controllo e monitoraggio che il software applicativo dovrà supportare.

### 4.2.1 Gestione degli Asset

Il sistema dovrà permettere di effettuare l'inventario di tutti i sistemi sottoposti a monitoraggio.
In particolare da questa funzionalità devono essere possibili almeno le seguenti azioni:

- gestione (aggiunta/modifica/cancellazione) di un apparato in modalità manuale;
- gestione massiva (aggiunta/modifica/cancellazione) di più apparati;
- discovery delle connessioni al livello 2 utilizzando i protocolli CDP e LLDP;

- discovery della rete al livello 3 utilizzando una community SNMP o un subset di indirizzi IP;
- gestione (aggiunta/modifica/cancellazione) dei contratti e delle licenze;
- visualizzazione grafica della topologia di rete al livello 2 e 3;
- visualizzazione dell'inventario completo di tutti i dettagli delle apparecchiature monitorate (ad esempio nome, chassis, moduli, interfacce).

### 4.2.2 Gestione delle configurazioni

Il sistema dovrà gestire le configurazioni degli apparati di rete, in particolare l'utente dovrà essere in grado di effettuare almeno le seguenti azioni:

- salvataggio automatico e\o manuale delle configurazioni;
- storicizzazione di almeno 10 configurazioni per ogni apparato;
- differenza tra due configurazioni dello stesso apparato;
- ricerca di stringhe all'interno delle configurazioni.

### 4.2.3 Monitoraggio

Il sistema dovrà permettere all'utente di identificare i problemi che possono occorrere sugli apparati e sulla rete, inoltre dovrà supportare i seguenti protocolli:

- SNMP (UDP/161);
- SNMP TRAP (UDP/162);
- Syslog;
- Netflow.

In particolare dovrà permettere almeno le seguenti azioni:

- monitoraggio dello stato degli apparati e della rete via ICMP e SNMP al fine di identificare problemi di disponibilità;
- visualizzazione dello stato degli apparati con differenti colori a seconda della gravità ;
- controllo proattivo dello stato della rete e gestione degli errori;
- controllo delle performance e dei livelli di servizio degli apparati e della rete;
- visualizzazione centralizzata degli errori e degli eventi in tempo reale con differenti colori a seconda della gravità;
- interrogazioni basate sul protocollo SNMP al fine di monitorare performance degli apparati (derivate o calcolate dalle informazioni delle MIB);
- visualizzazione di statistiche sugli errori e sulla disponibilità dei dispositivi monitorati;
- evidenziazione di situazioni anomale: il sistema deve essere in grado di analizzare i dati storici e evidenziare situazioni anomale confrontando i grafici di comportamento passati con quelli attuali.

Dalla visualizzazione degli eventi o dallo stato degli apparati dovrà essere possibile creare una segnalazione sul sistema informatico per la gestione dei ticket utilizzando le informazioni presenti nel sistema.

### 4.2.4 Troubleshooting

Il sistema dovrà garantire la risoluzione, in modo rapido e proattivo, dei problemi di rete prima che possano impattare sugli utenti finali o sui servizi attraverso la:

- diagnostica degli apparati di rete;

- verifica dei tempi di risposta degli apparati e di attraversamento della rete;
- analisi dei percorsi di livello 2 e di livello 3;
- analisi degli errori e degli eventi;
- correlazione di tutti gli eventi, quali anomalie di rete o guasti;
- definizione e configurazione di regole (basate su espressioni regolari) e azioni per le varie tipologie di eventi (ad esempio SMS, Email, eseguire script o comandi)
- analisi di flussi di rete NetFlow.

### 4.2.5 Reportistica

Dovrà essere possibile accedere a tutti i report da un unico punto, in modo da permettere la navigazione e l'accesso a report e informazioni dettagliate. In particolare dovrà essere possibile effettuare dei report sui seguenti beni: inventario, configurazioni, servizi, performance, utenti.

I report dovranno quindi essere facilmente programmabili per essere eseguiti in maniera schedulata oppure per essere visualizzati in tempo reale. Inoltre dovrà essere possibile esportarli in formato PDF o CSV.

Il sistema dovrà permettere la generazione, sia in maniera schedulata che manuale, di report personalizzabili dall'operatore sull'insieme delle informazioni presenti nella base dati

### 4.2.6 Amministrazione

L'utente del sistema dovrà essere in grado di poter gestire tutte le funzioni di amministrazione con particolare riferimento:

- alla gestione (inserimento/modifica/cancellazione) degli utenti su database locale;
- alla gestione (inserimento/modifica/cancellazione) di utenti attraverso server LDAP;
- alla gestione (inserimento/modifica/cancellazione) di gruppi di utenti;
- al controllo degli accessi e tracciamento delle azioni effettuate;
- all'autorizzazione e personalizzazione delle applicazioni e delle interfacce in base all'utente o al gruppo di utenti;
- ai parametri di configurazione del software applicativo.

# 5 SISTEMA INFORMATICO PER LA GESTIONE DEI TICKET

Nel presente capitolo sono riportati i requisiti minimi che dovranno obbligatoriamente essere rispettati e supportati nella soluzione proposta dal fornitore per la gestione dei ticket.
La soluzione dovrà essere del tipo "tutto incluso" e quindi completa di hardware, software di base e software applicativo.
L'hardware dovrà essere dimensionato in modo da garantire le esigenze espresse dall'Amministrazione e riportate nel paragrafo 2.1 e, parimenti, il software dovrà essere opportunamente corredato di licenze d'uso in modo da garantire la gestione di tutti i ticket per i quali l'Amministrazione richiede tale servizio.
In particolare il software applicativo, di tipo *Web-based*, e il sistema operativo dovranno essere basati su soluzioni open source e il fornitore dovrà rilasciare all'Amministrazione, tutto il codice sorgente delle parti software sviluppate ad hoc per l'integrazione delle diverse soluzioni, opportunamente commentato e documentato.
Per soluzioni open source si intendono tutte le soluzioni che hanno licenze approvate esplicitamente dalla OSI oppure considerate dalla FSF libere (free) o compatibili con la GPL.

Per le sue caratteristiche e le funzioni cui sarà preposto, il sistema dovrà inoltre consentire lo scambio delle informazioni il sistema di gestione della rete e deve essere un *framework* flessibile per la modellazione di processi con *workflow* applicativi su più livelli al fine di integrarsi con i flussi dell'Amministrazione.

## 5.1 Hardware

La fornitura dovrà prevedere un sistema hardware ridondato sul quale installare il software di base e applicativo in modo da garantire continuità di funzionamento a quest'ultimo in caso di guasto di un singolo componente. Di seguito vengono descritte le caratteristiche minime del sistema:

- apparato da rack;
- doppia alimentazione:
- sistemi di ventilazione adeguati alla potenza dissipata e ridondati;
- interfacce di rete 2x1Gbps e 1x10Gbps;
- storage in raid 1 (mirroring).

Il fornitore dovrà garantire e certificare la compatibilità tra la soluzione hardware e le soluzioni software adottate.

## 5.2 Funzionalità

Il sistema informatico dovrà fornire gli strumenti necessari per la creazione di segnalazioni di guasto o richieste d'intervento (ticket). All'interno dei singoli ticket sono contenute tutte le informazioni necessarie per la descrizione e la localizzazione del problema occorso e di uno o più dispositivi interessati.
Tali informazioni, sia statiche (informazioni acquisite al momento della sua creazione) che dinamiche (azioni e commenti inseriti nel corso del trattamento), saranno mantenute durante tutto il ciclo di vita.
Il sistema dovrà assegnare ad ogni ticket generato un ID univoco per permetterne l'individuazione e gestire l'intero ciclo di vita:

- creazione del ticket da parte dell'utente attraverso il sistema informatico per la gestione della rete oppure attraverso un'interfaccia del sistema informatico per la gestione dei ticket;
- identificazione del problema (assegnazione della priorità e selezione del LDS);
- assegnazione del ticket al personale suddiviso in differenti presidi tecnici o gruppi fornitore ;
- gestione dell'evoluzione del ticket (inserimento di ulteriori informazioni, gestione della priorità, modifica dello stato, ricerca ecc..); chiusura del ticket e segnalazione all'utente finale.

Il sistema, inoltre, dovrà prevedere la possibilità di integrazione con sistemi di trouble ticket di enti esterni.
Il monitoraggio dei ticket dovrà offrire la possibilità di coinvolgere livelli gerarchici o funzionali superiori e definire logiche di priorità in base al loro impatto ed urgenza.
Il sistema dovrà esser in grado di mantenere in linea, oltre ai ticket in lavorazione, almeno un mese solare dei ticket risolti e storicizzare almeno due anni solari. La funzionalità di ricerca dovrà essere possibile sia sulla quota parte in linea sia su quella storicizzata.
Di seguito viene riportato un elenco minimo di informazioni necessarie per l'identificazione del problema:

- operatore che ha in carico il ticket;
- utente che ha segnalato il guasto oppure referente locale per la problematica.
- anagrafica del bene (localizzazione, tipologia di apparato, configurazione hardware e software, ecc.);
- descrizione del problema o della richiesta;

- dati di registrazione chiamata: numero di chiamata, data ed ora di apertura/chiusura;
- priorità della chiamata in base alla gravità;
- documentazione dei passi risolutivi e delle soluzione del problema.

### 5.2.1 Reportistica

Dovrà essere possibile generare dei report in differenti formati (tabellare, grafico a torta o grafico a linea). I report potranno essere relativi a tutti ticket memorizzati nel sistema e potranno essere effettuati per visualizzare statistiche ad esempio non esaustivo in base alla priorità, al tempo di risoluzione, alla tipologia di apparati.

Inoltre dovrà essere possibile esportare i report in formato PDF o CSV.

### 5.2.2 Amministrazione

L'utente del sistema dovrà poter gestire tutte le funzioni di amministrazione del sistema informatico, quali:

- la gestione (inserimento/modifica/cancellazione) degli utenti su database locale;
- la gestione (inserimento/modifica/cancellazione) degli utenti attraverso server LDAP;
- la gestione (inserimento/modifica/cancellazione) di gruppi di utenti;
- il controllo degli accessi e tracciamento delle azioni effettuate;
- l'autorizzazione e personalizzazione delle applicazioni e delle interfacce in base all'utente o al gruppo di utenti;
- i parametri di configurazione del software applicativo.

# 6 SERVIZI

Al fine di assicurare la continuità e l'efficienza del servizio reso, il fornitore dovrà garantire l'installazione e la configurazione dei sistemi informatici (paragrafi 6.1 e 6.2), l'assistenza tecnica necessaria (paragrafo 6.3) per tutto il periodo di copertura del contratto, il supporto specialistico a consumo (paragrafo 6.4) e la formazione erogata in modalità di training on the job (paragrafo 6.5).
L'Amministrazione organizzerà un primo incontro con i responsabili del fornitore al fine di pianificare le attività successive. La data del kick-off meeting sarà assunta come data di inizio lavori.
L'attività operativa attuale non potrà essere interrotta se non per brevi intervalli di tempo e durante particolari orari, questo comporterà che tutte le attività che implicheranno un fermo del servizio di monitoraggio della rete dovranno essere preventivamente concordate con l'Amministrazione.

## 6.1 Installazione

La consegna degli apparati dovrà avvenire presso la sede indicata dall'Amministrazione al paragrafo 3.1, secondo le tempistiche definite nel capitolo 7, i materiali di risulta d'imballo saranno prelevati e smaltiti a cura del fornitore.
Sarà cura del fornitore fornire cavetteria, cablaggi e quant'altro necessario per la posa in opera e l'installazione di tutte le apparecchiature per la loro corretta configurazione nonché per l'eventuale cablaggio con sistemi e apparati esistenti e non oggetto del presente contratto.
L'installazione e il cablaggio dell'intera infrastruttura dovrà terminare secondo le tempistiche definite nel capitolo 7.

## 6.2 Configurazione

Al completamento della fase di installazione il fornitore dovrà procedere alle attività di configurazione dei sistemi informatici previsti in fornitura come descritto nei seguenti sottoparagrafi.
Il fornitore si impegnerà a nominare un responsabile tecnico incaricato di curare il coordinamento tecnico delle attività in fase di realizzazione e di migrazione, nonché di svolgere la funzione di unico referente nei confronti dell'Amministrazione.
Per le attività di configurazione dovrà esser fornito un gruppo di lavoro formato da figure professionali con conoscenza dei sistemi in argomento.
Nell'ambito delle prove finalizzate alla verifica funzionale, il fornitore dovrà redigere e consegnare, entro il termine delle attività di configurazione, un rapporto contenente l'articolazione delle prove per la verifica dei requisiti.
L'Amministrazione si riserva la facoltà di rivedere e modificare l'articolazione ed il tipo dei test proposti.
La fase di configurazione di entrambi i sistemi dovrà avvenire secondo le tempistiche definite nel capitolo 7.

### 6.2.1 Sistema informatico per la gestione della rete

Il fornitore, dovrà provvedere alle attività di *discovery* della rete e del conseguente popolamento del database con tutti gli apparati che dovranno essere sottoposti a monitoraggio e della migrazione di tutte le informazioni necessarie presenti nell'ambiente esistente.
Il fornitore dovrà eseguire le attività di configurazione relativamente al sistema di gestione installato tra cui:

- configurare il sistema di gestione per la "presa in carico" degli apparati attivi segnalati dall'Amministrazione (ad es: configurazione degli indirizzi IP puntuali o range di indirizzamento, community SNMP, etc...). In particolare devono essere inseriti almeno gli apparati riportati nel paragrafo 2.1 che rispondono al protocollo SNMP;
- installare le MIB appropriate alla gestione degli apparati secondo le alberature rilasciate dai produttori indicati nel paragrafo 2.1;
- configurare più livelli di utenza per le operazioni di gestione (ad es: utente, amministratore) e suddividerle in gruppi, secondo le direttive espresse dall'Amministrazione;
- organizzare il cruscotto grafico di gestione in maniera conveniente all'espletamento delle funzioni di monitoraggio, in accordo alle direttive espresse dall'Amministrazione;
- associare icone differenti ad apparati con funzionalità;
- configurare opportune regole (ad es: invio di mail) in seguito a particolari eventi di fault o di allarme, su indicazione dell'Amministrazione;
- configurare opportuni circuiti di correlazione che consentano di ricondurre una serie di fault ad un unico allarme principale, causa della serie di eventi;
- configurare più categorie di allarmi che consentano la gestione separata delle trap in funzione della diversa tipologia delle stesse (ad es: trap relative allo stato delle interfacce di rete, trap relative allo stato dei nodi di rete, etc…).

### 6.2.2 Sistema informatico per la gestione dei ticket

Il fornitore dovrà importare i ticket presenti nella piattaforma attualmente in uso, inoltre dovrà procedere alla personalizzazione del sistema secondo i flussi di lavoro che saranno indicati dall'Amministrazione anche sulla base di quelli attualmente esistenti ed eseguire le attività di configurazione relativamente al sistema di gestione installato tra cui:

- configurare più livelli di utenza per le operazioni di gestione (ad es: utente, amministratore) e suddividerle in gruppi, secondo le direttive espresse dall'Amministrazione;
- configurare i livelli di autorizzazione (approvazione – rifiuto);
- personalizzare i flussi di lavoro in accordo alle direttive espresse dall'Amministrazione
- creazione di reportistica personalizzata.
- configurare l'invio di mail quando il ticket viene assegnato a specifici gruppi.

### 6.2.3 Gruppo di lavoro

Il gruppo di lavoro dovrà essere composto da sistemisti esperti e specialisti di prodotto che abbiano almeno 5 anni di esperienza nell'ambito delle attività sistemistiche e di networking.
Al fine di assicurare un'adeguata copertura del servizio si richiede che il gruppo di lavoro sia costituito da figure professionali con conoscenze approfondite sulla soluzione di sicurezza oggetto della fornitura.
Le variazioni della composizione delle risorse professionali nel corso del progetto dovranno essere approvate dall'Amministrazione ed in ogni caso dovranno possedere qualifiche o competenze non inferiori a quelle previste nell'offerta tecnica presentata in sede di gara.

## 6.3 Assistenza e manutenzione evolutiva

Insieme ai sistemi informatici in fornitura dovrà essere fornito un servizio di assistenza e manutenzione evolutiva per un periodo pari a 36 (trentasei) mesi a decorrere dalla data di verifica di conformità, tale servizio dovrà essere attivo h24, sette giorni su sette, per 365 giorni l'anno.
Il servizio di assistenza richiesto consiste nel ripristino delle complete funzionalità, nella messa a disposizione di tutte le parti di ricambio in sostituzione e nell'esecuzione delle prove e dei controlli necessari a garantire il ripristino del pieno funzionamento degli apparati di proprietà dell'Amministrazione, entro i LDS indicati nel capitolo 7.
Il ripristino del sistema informatico dovrà avvenire a fronte di un guasto, blocco o altro inconveniente non bloccante, intendendosi per guasto qualsiasi anomalia funzionale che, direttamente o indirettamente, provochi l'interruzione o la non completa disponibilità delle funzionalità del sistema in questione o, in ogni caso, qualsiasi difformità del prodotto in esecuzione dalla relativa documentazione tecnica e manualistica d'uso.
Il fornitore, durante il periodo di validità contrattuale, dovrà effettuare il servizio di assistenza hardware e software secondo le modalità descritte nei seguenti paragrafi.

### 6.3.1 Gestione e assistenza

Sono comprese nel servizio di gestione e assistenza tutte le attività di:

- installazione dell'hardware e del software, la loro configurazione e personalizzazione;
- eventuali migrazioni delle informazioni, qualora non previste nel processo d'aggiornamento;
- allineamento dei sistemi hardware e software alle più recenti innovazioni tecnologiche rilasciate dal produttore, nonché attivazione di tutte le attività necessarie per prevenire potenziali guasti dei sistemi e ripristino del funzionamento a fronte di eventuali guasti al fine di assicurare la regolare erogazione del servizio. Va precisato che le attività di innovazione tecnologica, come pure quelle relative alle correzioni, si riferiscono essenzialmente alla capacità di mantenere aggiornato ed in regolare stato di funzionamento sia il software che il firmware dell'hardware. A seguito del rilascio, da parte del produttore, di un aggiornamento e/o di una correzione software, l'attività di assistenza dovrà essere svolta in sinergia con quella di gestione, per l'esecuzione ed il controllo delle operazioni di modifica e upgrade dei sistemi in esercizio.

- è responsabilità del fornitore garantire la compatibilità degli aggiornamenti proposti con la soluzione hardware e software fornita.

Dovranno essere previste, quindi, attività di assistenza preventiva (attività di assistenza atta a prevenire l'occorrenza di errori, malfunzioni e guasti) e di assistenza correttiva (attività di assistenza a seguito di segnalazioni di malfunzioni o guasti). Sono comprese in queste anche le attività volte al miglioramento o arricchimento funzionale, a seguito di migliorie decise e introdotte dal fornitore stesso che non comportano oneri contrattuali.
Il fornitore dovrà garantire la fornitura di *patch* e aggiornamenti durante il periodo di copertura del contratto, qualora sia applicabile deve permettere l'accesso gratuito al sito aziendale, dal quale sia possibile ricevere informazioni su nuove versioni e aggiornamenti dei prodotti hardware e software installati.
Un tecnico provvederà ad una prima analisi del problema, a raccogliere le informazioni essenziali per poterlo gestire nel modo più efficiente e rapido ed infine a stimare i tempi di intervento.

### 6.3.2 Modalità di esecuzione

Il servizio di assistenza dovrà prevedere l'attivazione da parte del fornitore di un numero telefonico di contatto, di un indirizzo email e di un TTS per la gestione dei guasti e malfunzionamenti di un apparato o di una componente di esso, attivo h24, sette giorni su sette, per 365 giorni l'anno. Entro la data di inizio dei servizi l'Amministrazione comunicherà alla società aggiudicataria dell'appalto i nominativi e i gruppi di lavoro abilitati all'apertura delle chiamate da parte dell'Amministrazione.
Si precisa che, ai fini della misurazione dei livelli di servizio, l'orario di inoltro della chiamata via telefono o dell'email da parte dell'Amministrazione è considerato il riferimento temporale di apertura del ticket.
Il fornitore inserirà tale richiesta nel proprio TTS evidenziandone il livello di servizio ed assegnando ad essa un identificativo che dovrà comunicare all'Amministrazione all'apertura del guasto. Il sistema di gestione dovrà garantire il tracciamento della richiesta (stato dell'intervento) in tutte le sue fasi, fino alla chiusura dell'intervento stesso.
Il fornitore dovrà utilizzare parti di ricambio nuove di fabbrica, identiche alle parti sostituite e, ove esistenti, prodotte dallo stesso costruttore delle apparecchiature. Le parti di ricambio, il ritiro e lo smaltimento dovranno essere fornite dalla società aggiudicataria dell'appalto senza alcun onere per l'Amministrazione.
Nel caso in cui, a fronte di un guasto di un apparato, il fornitore non sia provvisto della parte di ricambio richiesta per la riparazione, potrà, al fine di ripristinare il servizio, operare la sostituzione con un altro sistema (o con un'altra componente) avente le medesime caratteristiche ed in grado di ristabilire la corretta e completa funzionalità. Tale soluzione è da considerarsi sempre e comunque provvisoria e non svincola il fornitore dall'obbligo di fornire l'apparato (o la componente) necessario per la riparazione. Il fornitore dovrà quindi intervenire nuovamente per operare la corretta sostituzione entro e non oltre 15 giorni lavorativi dal ripristino temporaneo del servizio.

## 6.4 Supporto specialistico

Per tutta la durata del contratto, l'Amministrazione potrà richiedere l'erogazione a consumo di un numero di giornate di supporto specialistico fino ad un massimo di nr. 170 (centosettanta) giornate, che potranno essere utilizzate per la realizzazione di diverse attività su entrambi i sistemi informatici oggetto della fornitura. A titolo esemplificativo ma non esaustivo, ne sono riportate di seguito alcune:

- implementazione di nuove funzionalità derivanti da specifiche esigenze di evoluzione dei sistemi informatici non note al momento;
- stesura di procedure e politiche di sicurezza inerenti il funzionamento in esercizio dei nuovi sistemi informatici;

- realizzazione di integrazioni personalizzate tra i sistemi forniti e quelli presenti attualmente all'interno dell'infrastruttura di rete.

Il supporto specialistico potrà essere richiesto dall'Amministrazione mediante e-mail (PEC), dal lunedì al venerdì dalle ore 9.00 alle ore 18.00 e il sabato dalle ore 9.00 alle ore 13.00.
Il supporto specialistico dovrà essere erogato con i seguenti livelli di servizio:

- tempo di presa in carico, 1 (uno) giorno lavorativo dalla ricezione della richiesta: il fornitore dovrà prendere in carico la chiamata inviando una email di conferma alla persona di riferimento indicata dall'Amministrazione;
- tempo di intervento 5 (cinque) giorni solari dalla presa in carico: per intervento s'intende la presenza fisica della risorsa nella sede indicata nella chiamata.

Per l'espletamento delle suddette attività il fornitore dovrà avvalersi di personale esperto nella tecnologia oggetto di intervento (e comunque compresa nell'ambito della fornitura), ed in possesso di competenza ed esperienza su tematiche inerenti sia aspetti tecnologici sia aspetti di sicurezza informatica.
A seconda delle attività da svolgere, l'Amministrazione potrà richiedere che il personale sia in possesso di determinati requisiti e competenze professionali. A titolo esemplificativo ma non esaustivo di seguito vengo indicati alcuni dei requisiti professionali che di volta in volta potrebbero essere richiesti:

- almeno 5 anni di esperienza nella progettazione, e realizzazione di architetture di rete;
- esperienza comprovata di configurazione e tuning relativa alle componenti del sistema informatico oggetto di fornitura;
- almeno 5 anni di esperienza in materia di sicurezza informatica, con particolare riferimento alla componente organizzativa, per la progettazione/realizzazione di sistemi di monitoraggio e supervisione delle reti.

Il fornitore dovrà produrre, di volta in volta, quanto necessario per consentire all'Amministrazione di comprovare l'esistenza dei requisiti professionali richiesti.
Tutte le attività e gli interventi richiesti ed erogati saranno consuntivati mediante un'apposita relazione delle attività di Supporto Specialistico svolte, redatta a cura del fornitore ed accettata dall'Amministrazione, nella quale verranno indicati l'orario di inizio, l'oggetto e la durata dell'intervento stesso (mezza giornata o giornata intera a seconda della durata dell'intervento).

## 6.5 Formazione

Il fornitore dovrà erogare un servizio di formazione rivolto al personale tecnico dell'Amministrazione, o eventuale personale di società da questa designato, con lo scopo di fornire loro una adeguata conoscenza del sistema informatico offerto, tale da consentire la gestione delle apparecchiature e dei prodotti software previsti nell'ambito della fornitura.
La formazione dovrà essere volta all'approfondimento di temi riguardanti l'utilizzo e la gestione del sistema informatico oggetto di fornitura comprendendo le caratteristiche e le funzionalità salienti, con particolare riferimento alle configurazioni hardware e software adottate. Inoltre dovrà comprendere le comuni problematiche riscontrabili nell'implementazione della tecnologia nell'ambiente applicativo dell'Amministrazione.
Il fornitore dovrà erogare due sessioni di formazione della durata totale di 10 (dieci) giorni su tutte le componenti del sistema oggetto di fornitura, la prima sessione sarà di livello base (dedicata agli operatori) mentre la seconda di livello avanzato (dedicata agli amministratori). Inoltre dovrà provvedere alla fornitura della documentazione didattica per i discenti, sia su supporto cartaceo, sia su supporto elettronico.
Le sessioni di formazione verranno tenute presso un apposito locale, adeguatamente attrezzato, messo a disposizione dall'Amministrazione.
Le sessioni di formazione dovranno essere erogate, previo accordo con l'Amministrazione, entro un tempo massimo di 2 (due) mesi dalla data di accettazione della fornitura.

Il completo e corretto espletamento delle sessioni di formazione sarà certificato mediante apposita relazione sulla formazione svolta comprendente un questionario che indichi il livello di gradimento del corso da parte dei discenti, redatta a cura dell'Impresa di concerto con l'Amministrazione.
Il fornitore al termine di ogni sessione rilascerà ai partecipanti un attestato di partecipazione.

# 7 TEMPISTICHE E LIVELLI DI SERVIZIO

Si riepilogano di seguito le tempistiche caratterizzanti i servizi descritti nel capitolo 6.

- *Kick off meeting*: l'Amministrazione, nella persona del Direttore dell'Esecuzione del Contratto, provvederà ad indire tale incontro entro 5 giorni lavorativi dalla data di esecutività del contratto.
- Installazione e configurazione di base: entro 30 giorni solari dalla data dal *kick-off meeting*.
- Configurazione: entro 60 giorni solari dal termine della configurazione di base. Al termine di tale attività il fornitore dovrà presentare un piano di test per la verifica di conformità.
- Verifica di conformità: entro e non oltre 15 giorni dall'accettazione del piano di test.

Si riportano di seguito, suddivisi per le voci oggetto della fornitura e relativamente al periodo di erogazione del servizio riportato nel presente capitolato, i livelli di servizio minimi attesi.

**Tabella 2 - Livelli di Servizio**

| INDICATORE DEL SERVIZIO | VALORI DI SOGLIA | PERIODO DI OSSERVAZIONE |
|---|---|---|
| Tempistiche di progetto | Come da paragrafo 7 | Una tantum |
| Tempo di presa in carico delle richieste di assistenza | Tempo di presa in carico:<br>≤ 30 minuti nel 90% dei casi<br>≤ 2 ore nel restante 10% dei casi | Trimestrale |
| Servizi di assistenza (guasti bloccanti) | Tempo di ripristino dell'infrastruttura o del servizio:<br>≤ 4 ore solari nel 95% dei casi<br>≤ 8 ore solari nel restante 5% dei casi | Trimestrale |
| Servizi di assistenza (guasti non bloccanti) | Tempo di ripristino dell'infrastruttura o del servizio:<br>≤ 24 ore solari nel 90% dei casi<br>≤ 72 ore solari nel restante 10% dei casi | Trimestrale |

# 8 VERIFICA DI CONFORMITÀ

Per dare avvio alle operazioni di verifica finale, l'Amministrazione dovrà ricevere da parte del fornitore una formale comunicazione di approntamento al collaudo al termine della fase di configurazione (Capitolo 7). Tale comunicazione dovrà essere corredata da un Piano dei Test Funzionali.
Al fine di certificare la compatibilità tra la soluzione hardware e le soluzioni software adottate il fornitore dovrà produrre in sede di verifica di conformità la relativa dichiarazione.
Nel corso della verifica di conformità, la Commissione avrà la facoltà di eseguire verifiche aggiuntive e differenti da quanto indicato nel Piano dei Test. Inoltre, per facilitare le operazioni di collaudo, la Commissione potrà richiedere la presenza del DEC e di personale inviato dal fornitore.
All'atto dell'accettazione della fornitura, in caso di esito positivo della verifica di conformità, verrà redatto e sottoscritto dall'Amministrazione il verbale di collaudo ed accettazione, cui sarà allegato il documento rapporto di collaudo in cui sono tracciate le attività svolte durante il collaudo stesso.
La presenza di anomalie che, a giudizio dell'Amministrazione, per gravità o numerosità, non consentano lo svolgimento o la prosecuzione delle attività di collaudo provocherà la sospensione del collaudo stesso. La suddetta sospensione potrebbe comportare il mancato rispetto della data prevista di fine collaudo, per cause imputabili al fornitore. Le anomalie emerse in fase di collaudo devono essere rimosse entro il termine massimo di 15 giorni lavorativi.