ALLEGATO 4

CAPITOLATO TECNICO - LOTTO I

SOMMARIO

1 INTRODUZIONE 3

2 CARATTERISTICHE DELLA FORNITURA 4

3 DESCRIZIONE DEI SERVIZI OGGETTO DEL LOTTO I 5

3.1 SEDI DI FORNITURA 6

4 DESCRIZIONE DELLA FORNITURA 7

4.1 SERVIZI DI SICUREZZA E MONITORAGGIO 7

4.1.1 Gestione e Monitoraggio 7

4.1.2 Servizi on demand 9

4.1.3 Modello architetturale per l'erogazione dei servizi di sicurezza e monitoraggio 9

4.1.4 Requisiti del SOC 10

4.1.4.1 Requisiti infrastrutturali 10

4.1.4.2 Requisiti di controllo dell'infrastruttura 11

4.1.4.3 Requisiti organizzativi 11

4.1.4.4 Requisiti di supporto all'amministrazione 12

4.1.4.5 Requisiti del personale 14

4.1.4.6 Ulteriori Requisiti 15

4.2 SISTEMI DI SICUREZZA IT 16

4.2.1 Recesso di un sistema dal contratto 17

4.2.2 Inserimento di un sistema nel contratto 17

4.2.3 Lista dei sistemi in gestione 17

4.3 RESPONSABILE DELLA FORNITURA, ATTIVITÀ ESECUTIVE 17

4.3.1 Startup del servizio 17

4.3.2 gestione dei servizi On Demand 19

4.3.2.1 Richiesta di Servizi On Demand 19

4.3.2.2 Attività esecutive relative a successive attivazioni di servizi On Demand. 19

4.4 AGGIORNAMENTI SOFTWARE DEGLI APPARATI IN GESTIONE 20

5 LIVELLI DI SERVIZIO 22

5.1 CLASSI DI APPARATI 22

5.1.1 LdS1 – Disponibilità dei servizi 23

5.1.2 LdS2 – Tempestività della presa in carico dei ticket 24

5.1.3 LdS3 – Tempestività di lavorazione dei ticket 26

5.1.4 LdS4 – Rilevazione degli incidenti di sicurezza 28

5.1.5 LdS5 – Segnalazione di guasti hardware 30

6 PERIODO TRANSITORIO 31

6.1 AFFIANCAMENTO DI INIZIO ATTIVITÀ 31

6.2 AFFIANCAMENTO DI FINE FORNITURA 31

7 CERTIFICAZIONI DELL'IMPRESA 32

8 REQUISITI DI CONFORMITÀ DELL'INFRASTRUTTURA 33

1 INTRODUZIONE

Il presente Capitolato Tecnico disciplina gli aspetti tecnici della fornitura dei servizi necessari per l'erogazione dei Managed Security Services per la Corte dei conti (nel seguito indicata per comodità con Cdc) afferenti al **Lotto I - "Servizi di sicurezza e monitoraggio".**

Nel seguito del documento si ricorrerà più volte ad alcuni termini cui è attribuito il seguente significato:

- **Capitolato Tecnico**, il presente documento;
- **Amministrazione**, la Corte dei conti, "Cdc";
- **Committente**, la CONSIP S.p.A.;
- **Impresa**, l'Impresa aggiudicataria della gara, eventualmente mandataria di un RTI;
- **Fornitura**, quanto indicato nel capitolo 2, come **Oggetto di Fornitura**, e descritto dettagliatamente nel capitolo 4;
- **Infrastruttura di sicurezza**, l'insieme dei Sistemi e dei servizi correlati atti a garantire un'adeguata protezione delle informazioni e dei servizi erogati dai sistemi informativi della Cdc;
- **Sistema di sicurezza (o Sistema),** espressione architetturale di una o più funzionalità dell'Infrastruttura di sicurezza, per esempio firewall, IPS, VPN, ecc.; ogni Sistema può essere costituito da uno o più Componenti di Sicurezza;
- **Componente di sicurezza (o Componente)**, un qualunque elemento hardware o software (per esempio nodo firewall, licenza software, console di gestione, ecc.) dei Sistemi facenti parte dell'Infrastruttura di sicurezza;
- **Servizio/i**, il servizio o l'insieme dei servizi connessi alla Fornitura in oggetto;
- **MSS**, Managed Security Services**;**
- **SOC**, Security Operation Center;
- **SaaS**, Security as a Services.

2 CARATTERISTICHE DELLA FORNITURA

Il Committente ha inteso organizzare la presente iniziativa di acquisizione in maniera da rispondere in modo efficiente e flessibile alle esigenze attuali e future dell'Amministrazione in tema di servizi di sicurezza.

L'insieme dei Managed Security Services di cui la Cdc intende avvalersi, è stato suddiviso in due distinte macroattività.
La prima macroattività ha come obiettivo principale la conduzione dei sistemi (gestione e monitoraggio) e l'introduzione di nuovi servizi di sicurezza on demand atti a mantenerne la perfetta efficienza ed il costante allineamento con l'evoluzione tecnologica del mercato ICT coerentemente con gli obiettivi strategici dell'Amministrazione.

La seconda macroattività ha come obiettivo il controllo e la valutazione dello stato della sicurezza implementata presso l'Amministrazione e l'attivazione on demand di ulteriori forme di controllo specifiche qualora la Cdc ritenga opportuno approfondire dei contesti specifici della sicurezza del proprio patrimonio informativo.

In considerazione della particolare natura dell'insieme di attività che vanno a costituire i Managed security Services, questi sono stati articolati in due lotti mutuamente esclusivi.

Il presente Capitolato tecnico descriverà l'oggetto di fornitura relativo al **Lotto I - "Servizi di sicurezza e monitoraggio"** costituito da:

- Gestione e monitoraggio per attività di management, monitoring, troubleshooting e reporting;
- Servizi on demand richiesti a fronte di evoluzioni tecnologiche o all'emergere di nuove esigenze della Corte dei conti.

La durata massima prevista per la fornitura del Lotto I è fissata a 36 mesi a partire dalla data di "Dichiarazione di inizio servizio".

3 DESCRIZIONE DEI SERVIZI OGGETTO DEL LOTTO I

Di seguito sono descritti i servizi e le specifiche tecniche ed i requisiti relativi alla **Fornitura del Lotto I**:

- **Servizi di sicurezza e monitoraggio**, secondo quanto descritto al paragrafo 4.1;
- **Requisiti del SOC**, secondo quanto descritto al paragrafo 4.1.4.

Per l'erogazione dei servizi oggetto del presente capitolato tecnico, l'Impresa dovrà definire le seguenti figure professionali:

- **Responsabile del contratto**, ha la responsabilità di gestire e risolvere tutte le problematiche legate al corretto svolgimento del contratto (es. fatturazione, verifica del rispetto dei livelli di servizio, definizione e aggiornamento del Team di gestione e monitoraggio – di cui al successivo paragrafo 4.1.4.5) nonché delle eventuali variazioni dell'elenco delle componenti di sicurezza gestite e l'attivazione di nuovi servizi on demand.
- **Responsabile tecnico** per l'erogazione dei servizi, ha la responsabilità di coordinare dal punto di vista operativo tutte le attività legate ai servizi oggetto del presente capitolato tecnico e di essere il punto di riferimento per l'attivazione dei servizi on demand. Il Responsabile tecnico dovrà inoltre coordinare tutte le attività e produrre resoconti periodici, da presentare per discussione durante i SAL di progetto.

  I SAL, da tenere con cadenza mensile o su esplicita richiesta del Committente, riguarderanno almeno i seguenti argomenti:
  - dettaglio delle attività svolte e quelle ancora da svolgere;
  - eventuali problematiche insorte;
  - questioni aperte di carattere strategico/metodologico da sottoporre all'attenzione del Committente.

  A fronte di eventuali problematiche che dovessero presentarsi, il SAL dovrà comprendere anche le relative proposte di risoluzione e la relativa ripianificazione delle attività impattate.

L'impresa dovrà comunicare al Committente/Amministrazione il numero di telefono e l'e-mail con le quali contattare tali figure professionali il cui ruolo potrà essere assunto anche dalla medesima persona.

I servizi precedentemente elencati, avranno efficacia a decorrere dalla data riportata nella "Dichiarazione di inizio dei servizi" che sarà comunicata, tramite lettera formale, dal Committente al Fornitore entro il termine di 30 (trenta) giorni dalla data di stipulazione del contratto ed avranno termine trascorsi 36 (trentasei) mesi dalla data riportata nella "Dichiarazione di inizio dei servizi" stessa.

Il Responsabile del Contratto ed il Responsabile tecnico per l'erogazione dei servizi parteciperanno agli incontri mensili con il Committente per comunicare gli aggiornamenti sullo stato dei servizi erogati e per condividere ogni eventuale azione correttiva necessaria al rispetto dei livelli di servizio (LdS) previsti. Tali incontri avverranno almeno dieci giorni lavorativi successivi al mese da analizzare, in data da concordare via mail tra le parti.

3.1 SEDI DI FORNITURA

Le prestazioni oggetto del presente capitolato dovranno essere erogate presso il SOC remoto dell'Impresa. Inoltre, qualora eventuali problematiche lo rendano necessario, l'Impresa si fa onere di intervenire "on-site" presso le sedi della Corte dei conti. Di seguito viene riportato un elenco non esaustivo delle sedi principali della Corte dei conti:

- Roma – via Antonio Baiamonti, n. 25;
- Roma - via Atanasio Soldati, n.80 (La Rustica).

4 DESCRIZIONE DELLA FORNITURA

Di seguito è fornita una descrizione di massima dei servizi "core" costituenti il Lotto I - "Servizi di sicurezza e monitoraggio".

Il Fornitore prende atto che, nel corso dell'erogazione dei servizi, l'introduzione di nuove tecnologie a fronte delle evoluzioni in ambito ICT potrà comportare significative variazioni del contesto tecnologico di inizio fornitura e si impegna ad erogare i servizi richiesti adeguando le conoscenze del personale impiegato nell'erogazione dei servizi o inserendo nei gruppi di lavoro risorse con skill adeguato, senza alcun onere aggiuntivo per Consip/Amministrazione.

I servizi dovranno essere erogati per l'intera durata indicata da Consip operando sia con gli strumenti a supporto delle infrastrutture di Consip e/o dell'Amministrazione, sia con strumenti messi a disposizione dal Fornitore in adempimento alle obbligazioni contrattuali; l'uso di questi strumenti/servizi non produrrà oneri aggiuntivi per Consip/Amministrazione.

4.1 SERVIZI DI SICUREZZA E MONITORAGGIO

Nell'ambito dell'insieme di attività che definiscono il Lotto I - "Servizi di sicurezza e monitoraggio", la ***Gestione e Monitoraggio*** dei sistemi di sicurezza rappresenta il servizio fondamentale per l'individuazione e la prevenzione dei rischi derivanti gli attacchi informatici.

4.1.1 GESTIONE E MONITORAGGIO

La Gestione e Monitoraggio dovrà prevedere almeno i seguenti servizi di sicurezza (di seguito indicati a titolo esemplificativo ma non esaustivo):

- Gestione e monitoraggio degli apparati IDS/IPS;
- Gestione e monitoraggio degli apparati Firewall (stateful inspection, Next generation, UTM, Web Application, DB, etc);
- Gestione delle piattaforme di autenticazione forte (token server, One Time Password server, PKI server, etc) comprendente la gestione delle policy, degli utenti e dei loro privilegi;
- Gestione della piattaforma Antivirus e dei relativi client;
- Gestione, correlazione ed analisi proattiva degli eventi di sicurezza prodotti da tutte le piattaforme gestite;
- Attività di Troubleshooting di tipo:
    - sistemistico su eventuali malfunzionamenti degli apparati gestiti;
    - sistemistico a supporto di problematiche riscontrate da altri gruppi (es. reti, applicativi);
    - di sicurezza su eventuali attività anomale riscontrate in tempo reale.

Le attività relative alla gestione sono, in via indicativa e non esclusiva, le seguenti:

- Analisi, gestione, backup e restore delle configurazioni;
- Controllo e ottimizzazione delle prestazioni;
- Gestione, verifica, analisi e archiviazione dei log;
- Attività di Incident Management e di risposta agli attacchi informatici;
- Attività proattive a garanzia della sicurezza IT;
- Analisi d'impatto e capacity planning a fronte dell'evoluzione dei sistemi e dei servizi;
- Verifica continua del livello delle minacce IT, facendo anche riferimento alle principali fonti informative del settore;
- Stesura di documenti periodici sullo stato della sicurezza informatica in Corte dei conti;
- Gestione del ticketing verso eventuali fornitori esterni per quanto riguarda malfunzionamenti dei servizi e degli apparati di sicurezza (antivirus, antispam, firewall, ecc.);
- collaborazione con i responsabili Corte nella progettazione ed implementazione di soluzioni evolutive per la sicurezza delle infrastrutture e dei dati.

Le attività di conduzione operativa dei sistemi dovranno comprendere anche l'attività di monitoraggio dei sistemi di sicurezza e la gestione degli allarmi.
Il fornitore dovrà provvedere alla raccolta, verifica, correlazione, analisi e storicizzazione degli allarmi generati e delle informazioni raccolte dalle infrastrutture di sicurezza di cui dispone l'amministrazione. In particolare il fornitore dovrà:

- gestire gli allarmi tramite:
  - recupero delle informazioni generate dai sistemi di sicurezza dell'Amministrazione;
  - analisi e correlazione delle informazioni raccolte e presentazione mediante report di sintesi;
  - notifica immediata di eventi critici che impattino sulla sicurezza dell'ambiente informatico dell'Amministrazione;
  - assegnazione di differenti priorità agli eventi/allarmi e presentazione, per ogni notifica ricevuta, delle informazioni circa:
    - la sorgente, tipologia, descrizione, severità dell'evento/allarme;
    - l'impatto contestualizzato all'ambiente operativo della Corte;
    - l'istante temporale in cui l'evento si è verificato;
    - le procedure messe in atto per la risoluzione o mitigazione del problema.
  - comunicazione dei messaggi di allarme e degli eventi, per mezzo di:
    - trouble ticketing;
    - e-mail;
    - chiamata telefonica;
    - SMS.
- Archiviare e gestire i log di sicurezza; dovranno essere effettuate le seguenti attività:
  - storicizzare le informazioni (log) prodotte dai sistemi di sicurezza sui sistemi di archiviazione della Corte;
  - effettuare ricerche sulle informazioni inventariate mediante filtri e query personalizzabili.

Il dettaglio delle modalità operative del monitoraggio di sicurezza verrà concordato con l'Amministrazione.

4.1.2 SERVIZI ON DEMAND

Un'ulteriore componente, fondamentale per rendere realmente flessibile l'approccio alla sicurezza in forma di servizi, consiste nell'attivazione "***on demand***" sia di servizi richiesti a fronte di evoluzioni tecnologiche sia all'emergere di nuove esigenze dell'amministrazione. Alcuni esempi dei servizi attivabili possono essere (a titolo esemplificativo ma non esaustivo):

- URL/Content Filtering;
- Antivirus Gateway;
- Computer Emergency Response Team, volto a rispondere in caso di incidente informatico, sia ad attacchi in tempo reale che ad un analisi post incidente al fine di limitare o annullare i danni causati dallo stesso;
- Access and Identity Audit:
    - Monitoraggio delle transazioni effettuate da un utente, da un'applicazione web fino al database contenente i dati.
    - Monitoraggio dei ruoli e mansioni dipartimentali degli utenti al fine di avere una visione analitica degli accessi in base al principio del "Need To Know";
    - Reportistica inerente l'utilizzo di privilegi da parte degli utenti al fine di affinare le policy in vigore evidenziando l'effettivo utilizzo dei privilegi (eventualmente discordanti) ed eventuali utenti "dormienti".

4.1.3 MODELLO ARCHITETTURALE PER L'EROGAZIONE DEI SERVIZI DI SICUREZZA E MONITORAGGIO

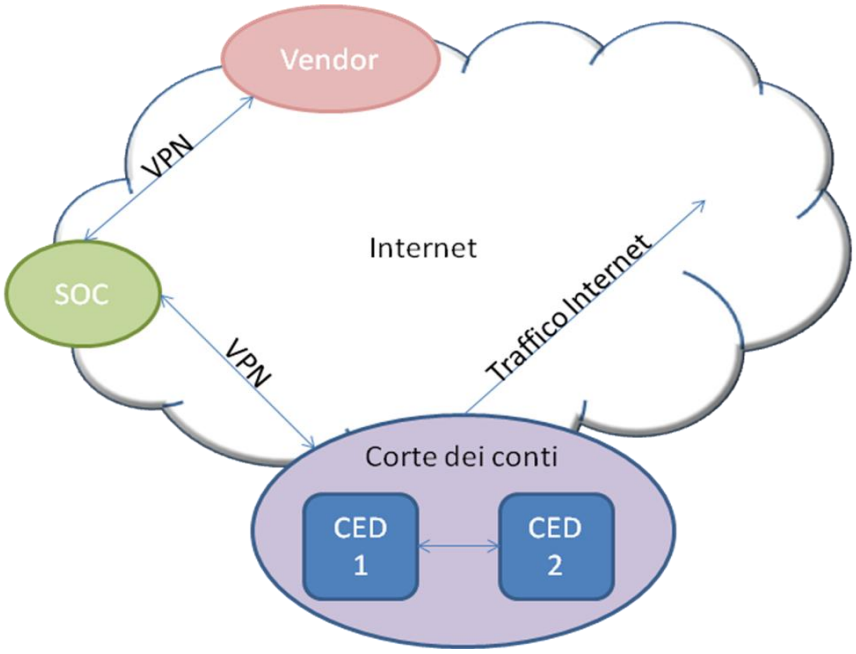
I servizi di sicurezza e monitoraggio verranno erogati dal Fornitore secondo un modello di "Remote Delivery" che prevede l'erogazione dei MSS attraverso un SOC dislocato geograficamente. Il *SOC* (che dovrà trovarsi all'interno del territorio nazionale) sfrutterà la propria connettività internet per attestarsi sulla rete di gestione Cdc attraverso un tunnel VPN di tipo site-to-site.

Il SOC si farà carico completamente degli oneri di gestione e monitoraggio dei servizi di sicurezza pur mantenendo i relativi apparati necessari all'erogazione di tali servizi all'interno del CED di Cdc.

I rapporti con i Vendor per le attività di manutenzione hardware e software, licensing e sostituzione degli apparati in caso di malfunzionamento, verranno gestite dal SOC attraverso la mediazione di Cdc.

Tale modello inoltre dovrà permettere l'attivazione on demand di alcuni servizi di sicurezza (come servizi di Content Filtering o Antivirus Gateway) che potranno essere richiesti da Cdc a fronte di evoluzioni tecnologiche delle proprie infrastrutture o dall'adozione di nuovi modelli di gestione della sicurezza.

Il SOC dovrà prevedere anche l'eventuale attivazione di servizi di tipo "Advanced Persistent Threat Prevention/Detection" per i quali potrà avvalersi del supporto di vendor specializzati.



4.1.4 REQUISITI DEL SOC

L'erogazione dei "Servizi di sicurezza e monitoraggio", presuppone che le attività che vanno a costituire la ***Gestione e Monitoraggio*** dei sistemi di sicurezza (comprendenti gli eventuali servizi on-demand) vengano svolte presso un SOC remoto. Per garantire la sicurezza delle informazioni e delle infrastrutture dell'Amministrazione è necessario stabilire dei requisiti minimi che dovrà possedere il Security Operation Center in termini sia infrastrutturali che organizzativi e gestionali.

4.1.4.1 Requisiti infrastrutturali

Tutte le infrastrutture utilizzate per l'erogazione dei servizi dovranno adottare le seguenti misure di carattere generale:

- Attuazione delle misure minime organizzative e tecniche previste dal Codice in materia di protezione dei dati personali (D.L. 30 giugno 2003, n. 196 Allegato B – Trattamento con strumenti elettronici);
- disposizione di un'organizzazione per la gestione della sicurezza dell'infrastruttura, secondo il modello indicato dalla norma BS7799-2;
- disposizione, nei punti di ingresso alle proprie infrastrutture utilizzate per l'erogazione dei servizi Cloud, di sistemi di controllo e filtraggio del traffico (firewall, IPS e liste di controllo di accesso a protezione degli apparati router) e di verifica

dell'assenza di codice malevolo nei messaggi di posta elettronica (sistema antimalware);
- implementazione di tutte le funzionalità necessarie ad impedire attacchi di tipo IP spoofing provenienti/diretti verso la rete dell'Amministrazione;
- garanzia di tempestivo aggiornamento, con applicazione delle patch, del software/firmware degli apparati (router-switch) che trasportano il traffico destinato all'Amministrazione;
- implementazione di un meccanismo di AAA centralizzato per l'autenticazione; l'autorizzazione e la tracciatura degli accessi sugli apparati utilizzati per l'erogazione dei servizi;
- tutti i sistemi che hanno impatti diretti o indiretti sull'erogazione del servizio all'Amministrazione dovranno essere ridondati così da garantire la continuità del servizio;
- il SOC dovrà prevedere un sito di disaster recovery.

4.1.4.2 Requisiti di controllo dell'infrastruttura

Per garantire la sicurezza e la continuità dei servizi erogati, il SOC dovrà aver implementato, su tutte le infrastrutture utilizzate per l'erogazione dei servizi, le seguenti misure di controllo:
- controllo costante dei propri apparati di rete e della rete fisica di trasporto con lo scopo di individuare eventuali anomalie che possano indicare problematiche di sicurezza;
- analisi automatica del traffico di rete con sistemi IDS/IPS con l'obiettivo di riconoscere potenziali attacchi;
- attivazione delle funzioni di tracciamento del traffico su tutti gli apparati di rete e sicurezza;
- definizione ed implementazione delle procedure di gestione degli incidenti a valle di segnalazioni di eventi di sicurezza.

I log relativi gli apparati di sicurezza volti alla protezione dei servizi erogati all'Amministrazione dovranno essere resi disponibili mensilmente (o su richiesta) sotto forma di reportistica all'Amministrazione stessa.

4.1.4.3 Requisiti organizzativi

Il Fornitore dovrà garantire che su tutte le infrastrutture utilizzate per l'erogazione dei servizi siano adottate le seguenti misure organizzative:
- analisi dei rischi su base sistematica, almeno con cadenza annuale. Tale analisi dovrà inoltre essere ripetuta a seguito di attacchi o incidenti gravi di sicurezza o per variazioni significative dell'architettura del SOC;
- verifica, con cadenza almeno semestrale, della capacità di resistenza dell'infrastruttura utilizzata per l'erogazione dei servizi nei confronti di attacchi esterni (vulnerability assessment);

- schedulazione di attività periodiche di revisione delle utenze e dei permessi ed immediata cancellazione delle utenze relative al personale che risolve il rapporto di lavoro;
- separazione delle responsabilità interne relative alla gestione della sicurezza ed alle verifiche;
- attivazione di un'organizzazione per la gestione dell'emergenza e dei problemi di sicurezza, volta ad assicurare la continuità del servizio nel caso di eventi eccezionali imprevedibili attraverso la stesura e la gestione dei piani per l'emergenza.

I risultati dei controlli effettuati sull'infrastruttura in oggetto e gli eventuali interventi correttivi dovranno essere messi a disposizione dell'Amministrazione in formato di reportistica sia elettronica che cartacea.

4.1.4.4 Requisiti di supporto all'amministrazione

Il Fornitore dovrà avvalersi del supporto di un Call Center quale punto di contatto sia per i servizi di provisioning (attivazione servizi, modifica policy, ecc.) sia per la gestione dei problemi che degli eventi di sicurezza.

La richiesta d'intervento (ticket) sarà attivato dal Committente/Amministrazione a terzi da essa designati, mediante chiamata telefonica ad un apposito Numero Verde e successivamente confermata via e-mail ad un indirizzo di posta elettronica, entrambi comunicati dall'Impresa.

Si precisa che l'ora di invio della e-mail da parte del Committente/Amministrazione a terzi da essa designati verrà considerata come l'ora di apertura del ticket.

In ogni caso l'Impresa dovrà dare comunicazione della presa in carico della richiesta di intervento inviando una e-mail ad un indirizzo all'uopo definito da Corte dei conti.
Quest'ultima e-mail dovrà contenere data ed ora di apertura della chiamata, identificativo (n° di intervento) della richiesta, i riferimenti relativi alla componente di sicurezza oggetto dell'intervento e una sintetica descrizione della richiesta di supporto.

L'impresa dovrà disporre di un sistema di gestione atto a garantire il tracciamento della chiamata (stato dell'intervento) in tutte le sue fasi fino alla chiusura della stessa.

Alla chiusura della chiamata sarà a carico del tecnico che ha eseguito l'intervento, la redazione di una nota d'intervento, associata ad un numero identificativo, da recapitare all'indirizzo sopra indicato, mediante il quale l'Impresa dovrà mantenere traccia delle azioni intraprese e consentire al Committente la verifica dell'attività svolta.
Tale nota d'intervento dovrà essere approvata dal Committente e dovrà contenere almeno le seguenti informazioni:

- numero identificativo della nota d'intervento;
- numero identificativo della chiamata;
- ora di inizio intervento (remoto);
- ora di inizio intervento on site (se effettuato);

- ora di chiusura intervento;
- nome del referente del Committente;
- descrizione dettagliata di quanto svolto;
- eventuali azioni correttive intraprese;
- esito della chiamata.

Il servizio di Call center dovrà ricevere segnalazioni di malfunzionamento almeno tramite i seguenti canali:

- chiamata telefonica attraverso un apposito Numero Verde;
- fax;
- e-mail;
- Portale Web.

Tale servizio dovrà essere disponibile in modalità 7x24x365 così da poter soddisfare tutti i livelli di servizio richiesti.

Il SOC dovrà includere una Base Dati contenente almeno le seguenti informazioni:

- ubicazione, tipologia e configurazione dei sistemi in gestione;
- policy configurate per ciascun sistema;
- misurazioni dei livelli di servizio che includono almeno i dati oggetto di tutti i report; periodici richiesti dall'amministrazione;
- log delle richieste di intervento pervenute al Call Center;
- log dei trouble ticket;
- classificazione dei guasti a seconda dei livelli di servizio contrattualizzati;
- dati di riscontro della qualità.

L'Impresa dovrà fornire visibilità all'Amministrazione dell'andamento dei servizi contrattualizzati, tali informazioni dovranno includere quelle sopraccitate.

Il SOC dovrà acquisire, da una sorgente primaria riconosciuta a livello Internazionale, il Tempo Ufficiale di Rete e utilizzarlo come riferimento temporale assoluto ai fini della marcatura con "time stamp" dei log e dei trouble tickets, nonchè per tutte le altre funzioni di gestione che richiedono un riferimento temporale.

Qualora l'amministrazione metta a disposizione i propri sistemi di gestione ticket, l'Impresa potrà avvalersi di questi al posto della modalità di gestione sopra descritta. Le attività propedeutiche all'utilizzo di tali sistemi (sviluppo software, connettività, etc) saranno a totale carico dell'Impresa.

4.1.4.5 Requisiti del personale

Di seguito vengono descritte, a titolo esemplificativo e non esaustivo, le figure professionali richieste:

Consulente specialista

- Almeno 7 anni di esperienza nella progettazione e realizzazione di progetti di sicurezza su tecnologie e architetture eterogenee;
- conoscenza approfondita del protocollo TCP/IP;
- conoscenza approfondita teorica e pratica delle problematiche di networking a livello 2 (Protocollo Spanning Tree, 802.1q trunking);
- esperienza nell'esecuzione di attività di troubleshooting a livello 2 e 3 con l'ausilio di strumenti di packet capture;
- conoscenza approfondita teorica a pratica dei protocolli di routing RIPv2 ed OSPF;
- conoscenza teorica dei protocolli di cifratura di livello 3 (IPSEC) e livello 7 (SSL) ed esperienza di configurazione dei relativi apparati di sicurezza;
- conoscenza approfondita delle principali tecnologie di network security (firewalling e Intrusion Prevention/Detection);
- esperienza nella realizzazione di architetture di sicurezza in ambienti con requisiti elevati di alta affidabilità e resilienza;
- conoscenza approfondita delle tecnologie di protezione Anti Virus di tipo endpoint e gateway;
- conoscenza approfondita delle principali tecnologie URL Filtering;
- conoscenza ed esperienza di configurazione di tecnologie avanzate anti-malware;
- esperienza di realizzazione di progetti di sicurezza in contesti multi utente con requisiti elevati di profilatura delle utenze;
- conoscenza dell'architettura di Dominio Windows;
- conoscenza dei principali sistemi operativi Unix e Linux;
- esperienza nella realizzazione di shell script per integrazione di componenti software.

Sistemista Senior

- Almeno 5 anni di esperienza nella progettazione e realizzazione di progetti di sicurezza su tecnologie e architetture eterogenee;
- conoscenza approfondita del protocollo TCP/IP;
- conoscenza approfondita teorica e pratica delle problematiche di networking a livello 2 (Protocollo Spanning Tree, 802.1q trunking);
- esperienza dimostrabile nell'esecuzione di attività di troubleshooting a livello 2
- conoscenza teorica dei protocolli di cifratura di livello 3 (IPSEC) ed esperienza di configurazione dei relativ apparati di sicurezza;

- conoscenza approfondita delle principali tecnologie di network security (firewalling e Intrusion Prevention/Detection);
- conoscenza approfondita delle tecnologie di protezione Anti Virus di tipo endpoint e gateway;
- conoscenza dell'architettura di Dominio Windows;
- conoscenza dei principali sistemi operativi Unix e Linux.

Sistemista

- Almeno 2 anni di esperienza nella progettazione e realizzazione di progetti di sicurezza su tecnologie e architetture eterogenee;
- conoscenza approfondita del protocollo TCP/IP;
- conoscenza approfondita teorica e pratica delle problematiche di networking a livello 2 (Protocollo Spanning Tree, 802.1q trunking);
- esperienza dimostrabile nell'esecuzione di attività di troubleshooting a livello 2;
- conoscenza teorica dei protocolli di cifratura di livello 3 (IPSEC) ed esperienza di configurazione dei relativi apparati di sicurezza;
- conoscenza approfondita delle principali tecnologie di network security (firewalling e Intrusion Prevention/Detection);
- conoscenza approfondita delle tecnologie di protezione Anti Virus di tipo endpoint e gateway;
- conoscenza dell'architettura di Dominio Windows;
- conoscenza dei principali sistemi operativi Unix e Linux.

Sistemista Junior

- conoscenza del protocollo TCP/IP;
- conoscenza delle problematiche di networking a livello 2 (Protocollo Spanning Tree, 802.1q trunking);
- conoscenza dei protocolli di cifratura di livello 3 (IPSEC);
- conoscenza delle principali tecnologie di network security (firewalling e Intrusion Prevention/Detection);
- conoscenza delle tecnologie di protezione Anti Virus di tipo endpoint e gateway;
- conoscenza dell'architettura di Dominio Windows.

Qualora l'Amministrazione lo richieda, l'Impresa dovrà presentare le certificazioni in possesso del team preposto all'erogazione dei servizi del presente capitolato.

4.1.4.6 Ulteriori Requisiti

Il perimetro interessato all'erogazione dei Servizi Gestiti di Sicurezza che tratterà, direttamente o indirettamente, informazioni appartenenti all'Amministrazione (log, policy, configurazioni, etc.) dovrà essere **certificato ISO 27001**. In ogni caso tutto il perimetro del

SOC dovrà essere conforme **allo standard ISO 27001**.

Le attività svolte presso il SOC remoto, nel loro complesso, sono classificabili in un insieme di operazioni, per lo più ripetitive e pianificabili pertanto tali operazioni dovranno essere regolamentate attraverso i **processi ITIL di "Service Support"** in particolare per quanto riguarda:

- Event managment;
- Incident management;
- Problem management;
- Change management;
- Release management;
- Configuration management.

Il Fornitore, nell'organizzazione proposta per l'erogazione dei servizi per i processi sopra citati, dovrà individuare un "Process Manager" responsabile, sia formalmente che funzionalmente, delle operazioni eseguite nell'ambito dei processi.

Il sistema di gestione della qualità del SOC remoto dovrà essere conforme alle norme della serie ISO 9000 e in particolare dovrà aver conseguito la **certificazione ISO 9001**.

Qualora l'Amministrazione lo ritenga necessario, potrà richiedere che vengano svolte sul SOC attività di Security Assessment da terze parti ad onere del fornitore dei servizi.

4.2 SISTEMI DI SICUREZZA IT

Nella seguente tabella vengono riportati i sistemi di sicurezza in dotazione dell'Amministrazione, con indicazione della tipologia, marca, modello, quantità ed eventuale configurazione in H.A.. Tale lista va considerata a titolo puramente esemplificativo e non esaustivo:

	Fortigate 3040B	2 (in HA)
FORTINET	Fortigate 1240B	2 (in HA)
	Fortigate 620B	2 (in HA)
	FortiWiFi 50B	6
	FortiWiFi 60B	3
	Fortigate 80c	5
	FortiAnalyzer 400b	1
	FortiManager 400b	1
	FortiAnalyzer 100b	1
	FortiManager 100	1
JUNIPER	Juniper Networks SA4000	2 (in HA)
RSA	RSAEnVision Appliance	2 (in HA)
	RSA SecureID Appliance	2 (in HA)
RADWARE	Radware AppXML	1

4.2.1 RECESSO DI UN SISTEMA DAL CONTRATTO

Per ogni tipo di sistema o componente di sicurezza, la cui gestione e monitoraggio è disciplinata dal presente capitolato è previsto il recesso dal servizio in ogni momento del periodo di efficacia del contratto. Il recesso deve essere formalizzato, mediante apposita comunicazione al Fornitore da parte del Committente. Ciò comporterà, dal mese successivo alla segnalazione, la detrazione del canone di spesa relativo alla apparecchiatura, dal canone globale del contratto di manutenzione.

4.2.2 INSERIMENTO DI UN SISTEMA NEL CONTRATTO

Ogni tipo di sistema o componente di sicurezza acquisito ex-novo dall'Amministrazione o già facente parte della sua infrastruttura di sicurezza deve poter essere inserito nel suddetto contratto di manutenzione in qualsiasi momento del periodo di efficacia del contratto.
Inoltre per ogni sistema o componente di sicurezza già inserito nel contratto di manutenzione con una determinata Classe (A, B) deve essere prevista solo ed esclusivamente su indicazione del Committente, la possibilità di cambiare la Classe stessa.
I cambiamenti sopra indicati non potranno essere rifiutati dall'Impresa e verranno richiesti dal Committente via e-mail al Responsabile del Contratto con 15 giorni di preavviso.

L'inserimento di un nuovo sistema o la modifica di una Classe associata ad un sistema già in manutenzione, comporterà dal mese successivo al momento della segnalazione l'aggiornamento del canone di spesa al canone globale del contratto.

4.2.3 LISTA DEI SISTEMI IN GESTIONE

Ogni mese, il responsabile tecnico del servizio durante i SAL mensili, di cui al precedente capitolo 3, dovrà consegnare al Committente la lista dei sistemi in gestione al fine di fornire ad esso le necessarie informazioni relative alla fatturazione del servizio erogato.

4.3 RESPONSABILE DELLA FORNITURA, ATTIVITÀ ESECUTIVE

Entro 5 (cinque) giorni solari dalla stipula del contratto, l'Impresa comunicherà alla Consip i nominativi del Responsabile del contratto, del Responsabile tecnico e del Process Manager dei processi che regolamentano le attività svolte presso il SOC remoto.

Le attività esecutive, a carico dell'Impresa, sono strumentali alla corretta messa in opera della Fornitura.

4.3.1 STARTUP DEL SERVIZIO

Lo startup del servizio avverrà a seguito dell'invio, da parte del Committente all'impresa, della lettera di "Dichiarazione di inizio dei servizi".
Nella Dichiarazione di inizio dei servizi sarà contenuto l'elenco dei sistemi da mettere in gestione con associati la configurazione (HA o nodo singolo, funzionalità attive su apparati

multifunzione) ed i livelli di servizio associati a ciascun sistema di sicurezza.

L'Impresa, entro un tempo massimo di **10 giorni solari**, dalla data di "Dichiarazione di inizio dei servizi" dovrà aver:

- predisposto il canale VPN necessario per la conduzione da remoto dei sistemi di sicurezza della Cdc;
- verificato che tutti i sistemi di sicurezza oggetto della fornitura siano raggiungibili dal SOC remoto;
- fornito la documentazione di startup.

La documentazione di startup del servizio dovrà essere composta dalle seguenti voci:

- Piano tecnico contenente:
  - Il dettaglio delle modalità operative del SOC;
  - Il dettaglio delle specifiche attività che verranno svolte su ogni sistema di sicurezza della Cdc preso in carico;
  - I processi che governano le attività svolte presso il SOC con il relativo responsabile dei processi (Process Manager);
  - La Dichiarazione di Rispondenza ai requisiti del SOC (come descritti nel paragrafo 4.1.4) corredata dalla oppurtuna documentazione a supporto (es. certificazione ISO 9001, certificazione ISO 27001, etc.).
- Composizione del Team di conduzione dei sistemi di sicurezza, di cui al precedente paragrafo 4.1.4.5, il nominativo del Responsabile del Contratto, di cui al precedente capitolo 3, il nominativo del Responsabile tecnico per l'erogazione dei servizi, di cui al precedente capitolo 3 e gli estremi telefonici e l'indirizzo e-mail per l'attivazione delle chiamate, di cui al precedente paragrafo 4.1.4.4
- Documenti di presa in carico dei sistemi, come di seguito descritto.

Per quanto riguarda i documenti di presa in carico dei sistemi sarà carico dell'Impresa eseguire una verifica puntuale dello stato di ogni sistema indicato dal Committente/Amministrazione e redigere per ognuno di essi un documento di presa in carico.

Nel documento di presa in carico l'Impresa deve riportare il livello degli aggiornamenti hardware e software e le eventuali segnalazioni di errore o parti guaste riscontrate sul sistema e dovrà dichiarare che nulla osta alla presa in carico del sistema stesso.

Nel caso in cui la suddetta verifica evidenziasse eventuali problemi/anomalie sui sistemi di sicurezza esaminati, l'Impresa dovrà comunicare al Committente/Amministrazione quali sono gli elementi che ostano alla presa in carico del sistema di sicurezza e all'avvio del servizio di conduzione. In tale situazione il Committente/Amministrazione, verificato quanto segnalato dall'Impresa, avvierà le azioni necessarie alla rimozione dei problemi.

Rimane comunque facoltà del Committente/Amministrazione richiedere all'Impresa la presa in carico del sistema nello stato in cui si trova al momento della verifica, considerando il risultato della verifica stessa quale stato accettabile di funzionamento del sistema e assumendolo come stato di riferimento per l'erogazione del servizio.

Qualora siano necessarie ulteriori attività a supporto dei servizi erogati come l'installazione di apparati presso i locali CED della Cdc oppure lo sviluppo di componenti software per

l'integrazione di sistemi di ticketing con quelli in uso presso l'Amministrazione, saranno considerati a totale onere dell'Impresa.

4.3.2 GESTIONE DEI SERVIZI ON DEMAND

Il Committente/Amministrazione si riserva di attivare ulteriori Servizi On Demand a seguito di sopravvenute esigenze di evoluzione/adeguamento dell'Infrastruttura di sicurezza. Le modalità di gestione delle relative Forniture sono descritte nei paragrafi successivi.

4.3.2.1 Richiesta di Servizi On Demand

Per effettuare una richiesta di servizi On Demand, il Committente/Amministrazione comunicherà all'Impresa:

- L'elenco dei nuovi servizi/funzionalità che si intendono attivare;
- i tempi massimi delle attività esecutive.

La Richiesta di Servizi On Demand avverrà mediante chiamata telefonica, seguita dall'invio di una e-mail ad un indirizzo indicato dall'Impresa. La data della suddetta e-mail costituirà il riferimento per il rispetto dei tempi esecutivi della Fornitura.

4.3.2.2 Attività esecutive relative a successive attivazioni di servizi On Demand.

L'Impresa, **entro 10 (dieci) giorni solari dalla data di ricezione dell'e-mail** di richiesta del Committente/Amministrazione, dovrà trasmettere una pianificazione delle attività e delle risorse professionali impiegate per la gestione del nuovo servizio.

Qualora, per l'erogazione del nuovo servizio, sia necessaria l'installazione di una componente di sicurezza (a totale onere dell'Impresa) presso i locali CED dell'Amministrazione, sarà cura dell'Impresa presentare il Piano dei lavori, contenente la pianificazione delle attività di consegna, di installazione e configurazione e delle risorse professionali impiegate in ciascuna fase, che dovrà essere approvato dal Committente.

Le attività esecutive dovranno rispettare le seguenti tempistiche:

- consegna: **entro massimo 20 (venti) giorni solari** dall'approvazione del Piano dei lavori;
- installazione e configurazione: **entro massimo 30 (trenta) giorni solari** dall'approvazione del Piano dei lavori.

L'Impresa potrà comunicare eventuali problematiche legate alla disponibilità dei beni/servizi, o alle modalità esecutive, richiedendo al Committente/Amministrazione l'estensione dei tempi massimi previsti. Qualora vengano concordate nuove tempistiche massime sulle fasi di realizzazione, queste dovranno essere approvate dal Committente/Amministrazione sul nuovo piano dei lavori presentato dall'Impresa.

Ultimata la fase di installazione e configurazione, **entro 5 (cinque) giorni solari**, l'Impresa dovrà produrre, il Rapporto di Fine Installazione, contenente almeno: marca, modello e

serial-number dell'apparato stesso.

Entro 5 (cinque) giorni solari dalla data del Rapporto di fine Installazione, l'Impresa dovrà presentare il Piano di Verifica, che dovrà essere approvato dal Committente, contenente tutti i casi di test da effettuare sugli apparati installati, per la verifica della corretta erogazione del servizio richiesto.

Una volta ultimata positivamente la verifica della corretta erogazione del servizio, secondo le attività descritte nel Piano di Verifica, **entro un massimo di 5 (cinque) giorni solari dalla data di approvazione del Piano di verifica**, l'Impresa, in contraddittorio con il Committente, dovrà produrre un Rapporto di Inizio servizio, la cui data sarà considerata come data di inizio di erogazione del servizio stesso.

4.4 AGGIORNAMENTI SOFTWARE DEGLI APPARATI IN GESTIONE

L'Impresa avrà l'onere di monitorare costantemente ed in maniera continuativa:

- il rilascio di aggiornamenti, di nuove versioni o correzione (hardware, software di base, software applicativo e firmware) rilasciate dai vendor dei rispettivi componenti di sicurezza gestiti;
- le scadenze delle licenze dei prodotti software installati sui componenti, lo stato di end of support (EoS) e lo stato di end of life (EoL) rilasciate dai produttori di tutti i sistemi di sicurezza oggetto della fornitura;

e darne pronta segnalazione al Committente/Amministrazione **entro un tempo massimo di 30 giorni precedenti dalla data di rilascio/comunicazione delle stesse**.

Inoltre, l'Impresa dovrà verificare e segnalare al Committente/Amministrazione, mediante un rapporto tecnico, la compatibilità e l'impatto tecnologico degli aggiornamenti, delle nuove versioni o delle correzioni con l'ambiente di esercizio **entro 20 giorni lavorativi dalla data della pubblicazione della notizia da parte dei vendor**, pena l'applicazione delle penali di cui allo schema di contratto.

Il rapporto tecnico sarà soggetto alla validazione da parte del Committente/Amministrazione che, in caso di esito positivo, deciderà i tempi e le modalità di intervento che l'impresa dovrà rispettare per rendere operative (installare, configurare e personalizzare) le modifiche segnalate, oppure di non procedere all'applicazione degli aggiornamenti segnalati.

In caso di esito negativo della valutazione del rapporto tecnico, segnalato a mezzo posta elettronica al Responsabile tecnico per l'erogazione dei servizi, l'Impresa dovrà produrre un nuovo rapporto tecnico **entro e non oltre 5 giorni lavorativi dalla data della segnalazione pena l'applicazione delle penali di cui allo schema di contratto**.

A fronte dell'acquisizione da parte del Committente/Amministrazione di nuove versioni dei software dei componenti di sicurezza, l'Impresa, su richiesta del Committente/Amministrazione, dovrà installare, configurare e personalizzare gli aggiornamenti.

Qualora, durante lo svolgimento della gestione dei sistemi, l'impresa riscontrasse dei malfunzionamenti nei componenti di sicurezza, dovrà comunicare tale evidenza al Committente/Amministrazione.

Inoltre l'Impresa dovrà provvedere ad effettuare tutte le attività necessarie a garantire il ripristino del pieno funzionamento dei sistemi di sicurezza nel rispetto dei livelli di servizio di cui al paragrafo 5.1.1.

Gli aggiornamenti software degli apparati in gestione fanno parte del servizio base "**Gestione e Monitoraggio**" e dovranno essere erogati dall'Impresa a propria cura e spese, senza alcun onere aggiuntivo per l'Amministrazione.

5 LIVELLI DI SERVIZIO

Il livello di servizio (LdS) assegnato ad un particolare sottosistema potrà essere modificato su richiesta del Committente in un qualsiasi momento del periodo di efficacia del contratto.

I livelli di servizio (LdS) per il Lotto I - servizi di Gestione e Monitoraggio saranno divisi nelle seguenti tipologie:

- Disponibilità dei servizi;
- Tempestività della presa in carico dei Ticket;
- Tempestività di lavorazione dei Ticket;
- Rilevazione degli incidenti di sicurezza;
- Segnalazione di guasti hardware.

5.1 CLASSI DI APPARATI

Per ogni sistema di sicurezza, gestito all'interno della presente fornitura, sarà assegnata una Classe che definirà i tempi e le modalità di erogazione del servizio di **"Gestione e Monitoraggio"**. Le due Classi che potranno essere assegnate agli apparati di sicurezza della Cdc, sono le seguenti:

Classe A: il servizio dovrà essere erogato 7 giorni la settimana per 24 ore al giorno 365 giorni l'anno.

Classe B: il servizio dovrà essere erogato dal lunedì al venerdì dalle ore 8:00 alle ore 20:00 (esclusi festivi).

Oltre alle tempistiche sopra esposte il LdS1 – Disponibilità dei servizi (di cui al paragrafo 5.1.1) e il LdS5 – Segnalazione dei guasti hardware (di cui al paragrafo 5.1.5), avranno ulteriori discriminanti in base alle classi degli apparati gestiti.

5.1.1 LDS1 – DISPONIBILITÀ DEI SERVIZI

I tempi di disponibilità effettiva del singolo servizio vengono calcolati sottraendo ai tempi di indisponibilità rilevati quelli non direttamente imputabili al servizio specifico o a servizi da cui lo stesso dipende.

Aspetto da valutare	Disponibilità dei servizi raggruppati in base alla Classe (*) • Classe A • Classe B		
Unità di misura	Punto percentuale	**Fonte dati**	Sistema di monitoraggio
Periodo di riferimento	Mese precedente la rilevazione	**Frequenza di misurazione**	Mensile
Dati elementari da rilevare	• Tempo di disponibilità effettiva dei servizi appartenenti ad un singola Classe *[Disponibilità_effettiva_servizi_(Classe_X)]* • Tempo di disponibilità richiesta dei servizi appartenenti ad un singola Classe *[Disponibilità_richiesta_servizi(Classe_X)]*		
Formule	$\mathbf{LdS1a} = \frac{\mathbf{Disponibilità_effettiva_Servizi_(Classe_A)}}{\mathbf{Disponibilità_richiesta_Servizi_(Classe_A)}}\mathbf{x100}$ $\mathbf{LdS1b} = \frac{\mathbf{Disponibilità_effettiva_Servizi_(Classe_B)}}{\mathbf{Disponibilità_richiesta_Servizi_(Classe_B)}}\mathbf{x100}$		
Valore di soglia	LdS1a >= 98,80% LdS1b >= 98,00%	**Valore di soglia migliorativo**	LdS1a >= 99,30% LdS1b >= 98,50%
Azioni contrattuali	▪ Mancata erogazione di quota parte del corrispettivo maturato legata all'indicatore di prestazione *"Gestione e monitoraggio"* qualora non sia rispettato il valore di soglia migliorativo ▪ Applicazione di una penale qualora non sia rispettato il valore di soglia		
Eccezioni	Le penali non sono applicabili nel periodo transitorio		

5.1.2 LdS2 – Tempestività della presa in carico dei ticket

Aspetto da valutare	Rispetto dei tempi di presa in carico dei ticket stabiliti in base all'urgenza della richiesta: • Critica • Alta • Media • Bassa Vanno considerati tutti i ticket che hanno la data di "assegnato" appartenente al periodo di riferimento		
Unità di misura	Punto percentuale	**Fonte dati**	Sistema di tracciatura dei trouble-ticket
Periodo di riferimento	Mese precedente la rilevazione	**Frequenza di misurazione**	Mensile
Dati elementari da rilevare	• Data in formato giorno-mese-anno ore-minuti di presa in carico (stato = "in corso") del singolo Ticket *[Data stato "in corso"]* • Data in formato giorno-mese-anno ore-minuti assegnazione (stato = "assegnato") del singolo Ticket *[Data stato "assegnato"]* • Numero dei ticket presa in carico di Urgenza Critica *[Ticket Urg_Critica_presa in carico]* • Numero dei ticket presa in carico di Urgenza Alta *[Ticket Urg_Alta_presa in carico]* • Numero dei ticket presa in carico di Urgenza Media *[Ticket Urg_Media_presa in carico]* • Numero dei ticket presa in carico di Urgenza Bassa *[Ticket Urg_Bassa_presa in carico]* • Numero totale dei ticket assegnati di Urgenza Critica *[Totale Ticket Urg_Critica_assegnati]* • Numero totale dei ticket assegnati di Urgenza Alta *[Totale Ticket Urg_Alta_assegnati]* • Numero totale dei ticket assegnati di Urgenza Media *[Totale Ticket Urg_Media_assegnati]* • Numero totale dei ticket assegnati di Urgenza Bassa *[Totale Ticket Urg_Bassa_assegnati]*		
Formule	T_presa_carico = Data stato "in corso" – Data stato "assegnato" $\mathrm{LdS2a} = \frac{\mathrm{Ticket_Urg_Critria_presa_in_carico}(T_\mathrm{presa_carico} <= 15')}{\mathrm{Totale_Ticket_Urg_Critica_assegati}} x100$ $\mathrm{LdS2b} = \frac{\mathrm{Ticket_Urg_Alta_presa_in_carico}(\mathrm{T_presa_cario} <= 30')}{\mathrm{Totale_Ticket_Urg_Alta_assegati}} x100$ $\mathrm{LdS2c} = \frac{\mathrm{Ticket_Urg_Media_presa_in_carico}(\mathrm{T_presa_cario} <= 60')}{\mathrm{Totale_Ticket_Urg_Media_assegati}} x100$ $\mathrm{LdS2d} = \frac{\mathrm{Ticket_Urg_Bassa_presa_in_carico}(\mathrm{T_presa_cario} <= 90')}{\mathrm{Totale_Ticket_Urg_Bassa_assegati}} x100$		

Valore di soglia	LdS2a >= 90,0% LdS2b >= 90,0% LdS2c >= 90,0% LdS2d >= 90,0%	**Valore di soglia migliorativo**	LdS2a >= 95,0% LdS2b >= 95,0% LdS2c >= 95,0% LdS2d >= 95,0%
Azioni contrattuali	▪ Mancata erogazione di quota parte del corrispettivo maturato legata all'indicatore di prestazione *"Gestione e monitoraggio"* qualora non sia rispettato il valore di soglia migliorativo ▪ Applicazione di una penale qualora non sia rispettato il valore di soglia		
Eccezioni	Le penali non sono applicabili nel periodo transitorio		

5.1.3 LDS3 – TEMPESTIVITÀ DI LAVORAZIONE DEI TICKET

Aspetto da valutare	Rispetto dei tempi di risoluzione dei ticket stabiliti in base all'urgenza(*) della richiesta: • Critica • Alta • Media • Bassa Vanno considerati tutti i ticket che hanno la data di "in corso" appartenente al periodo di riferimento		
Unità di misura	Punto percentuale	**Fonte dati**	Sistema di tracciatura dei trouble-ticket
Periodo d--i riferimento	Mese precedente la rilevazione	**Frequenza di misurazione**	Mensile
Dati elementari da rilevare	• Data in formato giorno-mese-anno ore-minuti di presa in carico (stato = "in corso") del singolo Ticket *[Data stato "in corso"]* • Data in formato giorno-mese-anno ore-minuti fine esecuzione (stato = "risolto") del singolo Ticket *[Data stato "risolto"]* • Numero dei ticket risolti di Urgenza Critica *[Ticket_ Urg_Critica_risolti]* • Numero dei ticket risolti di Urgenza Alta *[Ticket_Urg_Alta_risolti]* • Numero dei ticket risolti di Urgenza Media *[Ticket_Urg_Media_risolti]* • Numero dei ticket risolti di Urgenza Bassa *[Ticket_Urg_Bassa_risolti]* • Numero totale dei ticket risolti di Urgenza Critica *[Totale_Ticket Urg_Critica_Risolti]* • Numero totale dei ticket risolti di Urgenza Alta *[Totale_Ticket Urg_Alta_Risolti]* • Numero totale dei ticket risolti di Urgenza Media *[Totale_Ticket Urg_Media_Risolti]* • Numero totale dei ticket risolti di Urgenza Bassa *[Totale_Ticket Urg_Bassa_Risolti]*		

<table>
<tr><td>Formule</td><td colspan="3">T_risoluzione = Data stato “risolto” – Data stato “in corso”
$$LdS3a = \frac{Ticket_Urg_Critica_Risolti_(T_risoluzione <= 6h)}{Totale_Ticket_Urg_Critica_Risolti} x100$$
$$LdS3b = \frac{Ticket_Urg_Alta_Risolti_(T_risoluzione <= 8h)}{Totale_Ticket_Urg_Alta_Risolti} x100$$
$$LdS3c = \frac{Ticket_Urg_Media_Risolti_(T_risoluzione <= 12h)}{Totale_Ticket_Urg_Media_Risolti} x100$$
$$LdS3d = \frac{Ticket_Urg_Bassa_Risolti_(T_risoluzione <= 16h)}{Totale_Ticket_Urg_Bassa_Risolti} x100$$</td></tr>
<tr><td>Valore di soglia</td><td>LdS3a >= 90,0%
LdS3b >= 90,0%
LdS3c >= 90,0%
LdS3d >= 90,0%</td><td>Valore di soglia migliorativo</td><td>LdS3a >= 95,0%
LdS3b >= 95,0%
LdS3c >= 95,0%
LdS3d >= 95,0%</td></tr>
<tr><td>Azioni contrattuali</td><td colspan="3">▪ Mancata erogazione di quota parte del corrispettivo maturato legata all’indicatore di prestazione “Gestione e monitoraggio” qualora non sia rispettato il valore di soglia migliorativo
▪ Applicazione di una penale qualora non sia rispettato il valore di soglia</td></tr>
<tr><td>Eccezioni</td><td colspan="3">Le penali non sono applicabili nel periodo transitorio</td></tr>
</table>

5.1.4 LDS4 – RILEVAZIONE DEGLI INCIDENTI DI SICUREZZA

Nel caso di rilevazione di attività ostili, l'Impresa dovrà analizzare i relativi allarmi, al fine di discriminare i falsi positivi, e se necessario aprire un ticket di Incidente di Sicurezza.

Gli Incidenti di Sicurezza confermati e su cui sono richieste delle azioni, dovranno essere portati all'attenzione del referente del Committente/Amministrazione a terzi da essa designati per via mail oppure via telefonica, a seconda della gravità dell'evento.

L'Impresa dovrà fornire una descrizione dell'Incidente di Sicurezza, del suo potenziale impatto e una raccomandazione sulle azioni da intraprendere (es. modifiche alle policy).
L'Impresa dovrà identificare l'Incidente di Sicurezza con il relativo livello di Priorità: 1, 2 o 3 a seconda della gravità dell'evento.

In base al Livello di gravità dell'incidente occorso i tempi di reazione dovranno essere i seguenti:

- Priorità 1: apertura del ticket di Incidente di Sicurezza entro 15 minuti (solari) dall'identificazione dell'evento pena l'applicazione delle penali di cui allo schema di contratto. Qualora sia necessario intraprendere azioni per far fronte all'evento di sicurezza, parallelamente all'apertura del ticket, il referente del Consip/Cdc dovrà essere informato direttamente tramite mail o riferimento telefonico.
- Priorità 2: apertura del ticket di Incidente di Sicurezza entro 30 minuti (solari) dall'identificazione dell'evento pena l'applicazione delle penali di cui allo schema di contratto.
- Priorità 3: apertura del ticket di Incidente di Sicurezza entro 40 minuti (solari) dall'identificazione dell'evento pena l'applicazione delle penali di cui allo schema di contratto.

Aspetto da valutare	Rispetto dei tempi di segnalazione degli incidenti di sicurezza in base al livello di priorità: • Priorità 1 • Priorità 2 • Priorità 3 Vanno considerati tutti gli incidenti che hanno la data appartenente al periodo di riferimento		
Unità di misura	Punto percentuale	**Fonte dati**	Sistema di tracciatura dei trouble-ticket/mail
Periodo di riferimento	Mese precedente la rilevazione	**Frequenza di misurazione**	Mensile

Dati elementari da rilevare	• Data in formato giorno-mese-anno ore-minuti dell'inizio dell'incidente di sicurezza(stato = "incidente in corso") • Data in formato giorno-mese-anno ore-minuti della segnalazione dell'incidente (stato = "incidente segnalato") • Numero degli incidenti di sicurezza di Priorità 1*[Totale incidenti priorità1]* • Numero degli incidenti di sicurezza di Priorità 2*[Totale incidenti priorità2]* • Numero degli incidenti di sicurezza di Priorità 3*[Totale incidenti priorità3]*		
Formule-	T_segnalazione_incidente = Data stato "inizio incidente" – Data stato "incidente segnalato" $\text{LdS4a} = \frac{\text{Segnalazione_Incidente_Sicurezza_Priorità_1}(T\text{_segnalazione_inciden}}{\text{Totale_incidenti_priorità_1}}$ $\text{LdS4b} = \frac{\text{Segnalazione_Incidente_Sicurezza_Priorità_2}(T\text{_segnalazione_inciden}}{\text{Totale_incidenti_priorità_2}}$ $\text{LdS4c} = \frac{\text{Segnalazione_Incidente_Sicurezza_Priorità_3}(T\text{_segnalazione_inciden}}{\text{Totale_incidenti_priorità_3}}$		
Valore di soglia	LdS5a >= 95,0% LdS5b >= 95,0%	**Valore di soglia migliorativo**	LdS5a >= 98,0% LdS5b >= 98,0%
Azioni contrattuali	▪ Mancata erogazione di quota parte del corrispettivo maturato legata all'indicatore di prestazione **IP1** "*Qualità del Servizio di Supporto*" qualora non sia rispettato il valore di soglia migliorativo ▪ Applicazione di una penale qualora non sia rispettato il valore di soglia		
Eccezioni	Le penali non sono applicabili nel periodo transitorio		

5.1.5 LdS5 – Segnalazione di guasti hardware

Qualora si verifichi un disservizio causato da un guasto hardware l'impresa dovrà aprire un ticket di guasto hardware e comunicare l'evento al responsabile Consip/Cdc. I tempi previsti per l'apertura del ticket seguono le stesse modalità indicate per il *LdS1 – Disponibilità dei servizi* (paragrafo 5.1.1) in particolare i tempi previsti per l'apertura del ticket di guasto hardware dovranno rispettare le seguenti tempistiche:

Classe A: Apertura del ticket di guasto hardware entro 30 minuti solari dall'avvenuto disservizio.

Classe B: Apertura del ticket di guasto hardware entro 30 minuti lavorativi dall'avvenuto disservizio.

Aspetto da valutare	Rispetto dei tempi di segnalazione di guasti hardware in base alla Classe: • Classe A • Clase B Vanno considerati tutti i guasti che hanno la data appartenente al periodo di riferimento		
Unità di misura	Punto percentuale	**Fonte dati**	Sistema di tracciatura dei trouble-ticket
Periodo di riferimento	Mese precedente la rilevazione	**Frequenza di misurazione**	Mensile
Dati elementari da rilevare	• Data in formato giorno-mese-anno ore-minuti dell'inizio del guasto Hardware (stato = "guasto in corso") • Data in formato giorno-mese-anno ore-minuti della segnalazione (stato = "guasto segnalato") • Numero dei guasti hardware delle componenti di sicurezza di Classe A*[Totale guasti sistemi classe A]* • Numero dei guasti hardware delle componenti di sicurezza di Classe B*[Totale guasti sistemi classe B]*		
Formule	T_segnalazione_guasto = Data stato "guasto in corso" – Data stato "guasto segnalato" $\text{LdS5a} = \frac{\text{Segnalazione_Guasto_Sistema_Classe_A}(T_\text{segnalazione_guasto} <= 30')}{\text{Totale_guasti_sistemi classe_A}} x100$ $\text{LdS5b} = \frac{\text{Segnalazione_Guasto_Sistema_Classe_B}(T_\text{segnalazione_guasto} <= 30')}{\text{Totale_guasti_sistemi classe_B}} x100$		
Valore di soglia	LdS5a >= 90,0% LdS5b >= 90,0%	**Valore di soglia migliorativo**	LdS5a >= 95,0% LdS5b >= 95,0%
Azioni contrattuali	▪ Mancata erogazione di quota parte del corrispettivo maturato legata all'indicatore di prestazione **IP1** *"Qualità del Servizio di Supporto"* qualora non sia rispettato il valore di soglia migliorativo ▪ Applicazione di una penale qualora non sia rispettato il valore di soglia		
Eccezioni	Le penali non sono applicabili nel periodo transitorio		

6 PERIODO TRANSITORIO

Nei primi tre mesi dall'inizio delle attività il non raggiungimento dei valori di soglia previsti dai livelli di servizio non sarà soggetto all'applicazione di penali o alla formalizzazione di rilievi ma inciderà sul conseguimento degli obiettivi di prestazione a cui è legata una quota della prestazione. Il Fornitore deve essere comunque impegnato al raggiungimento dei livelli previsti. Ogni eventuale scostamento dalle soglie previste dovrà essere motivato e dettagliato.
Durante tale periodo al Fornitore verrà riconosciuto il corrispettivo indicato nello schema di contratto.

6.1 AFFIANCAMENTO DI INIZIO ATTIVITÀ

Entro cinque giorni lavorativi dalla stipula del contratto, per una **durata massima di 30 giorni** solari e comunque entro la data di inizio attività, il Fornitore dovrà effettuare l'affiancamento agli attuali fornitori dei servizi richiesti onde acquisire le conoscenze necessarie al corretto svolgimento dei servizi richiesti o per collaborare alla soluzione di eventuali problemi di particolare rilevanza.
Si precisa che l'eventuale riduzione del periodo di affiancamento iniziale sarà applicata alla presa in carico di tutte le attività affidate nell'ambito del contratto.
Per tutto il periodo di affiancamento di inizio fornitura, il Fornitore non percepirà alcun corrispettivo per le attività ed i servizi oggetto della presa in carico.
In merito all'affiancamento di inizio fornitura, si precisa che il Committente/Amministrazione fornirà la documentazione tecnica (manualistica, reportistica periodica, ecc.) e illustrerà le metodologie ed i processi relativi all'erogazione dei servizi.
Il passaggio di know how potrà avvenire attraverso sessioni riassuntive, sessioni di lavoro congiunto, presentazioni, tavole rotonde e consegna di documentazione.

6.2 AFFIANCAMENTO DI FINE FORNITURA

Negli **ultimi 2 mesi di validità del contratto** o nel caso di cessazione anticipata del rapporto contrattuale, il Fornitore dovrà, su richiesta del Committente/Amministrazione, fornire a personale del Committente/Amministrazione o a terzi da essa designati il trasferimento del know-how sulle attività condotte, al fine di rendere l'eventuale prosecuzione delle attività quanto più efficace possibile.
Tale periodo di affiancamento sarà organizzato secondo modalità da concordare e potrà prevedere sessioni riassuntive, sessioni di lavoro congiunto, presentazioni, tavole rotonde, ecc.
Al fine di facilitare il trasferimento del know how sarà stilata una lista delle attività di dettaglio da effettuare che sarà sottoposta all'approvazione del Committente e/o all'Amministrazione. L'onere di predisposizione di tale lista è a carico del Fornitore.

7 CERTIFICAZIONI DELL'IMPRESA

L'Impresa dovrà dimostrare, producendo tutta la relativa documentazione (anche in autocertificazione), la sussistenza dei requisiti per il rispetto delle seguenti normative:

- DPR. 27/04/1955 n. 547 e DPR. 07/01/1956, sull'osservanza da parte dei singoli lavoratori delle norme di sicurezza citate e sull'uso dei mezzi di protezione messi a loro disposizione;
- DPR. 19/03/1956 n. 303, Norme Generali per l'igiene del lavoro;
- D.Lgs. 19 settembre 1994 N. 626, attuazione direttive CEE riguardanti il miglioramento della sicurezza e della salute dei lavoratori sul luogo di lavoro e successivi aggiornamenti;
- Legge n. 46 del 05/03/1990: norme sulla sicurezza degli impianti e relativo DPR 447/91 di attuazione, per quanto attiene alla installazione dei Componenti.

All'Impresa viene inoltre richiesto che le apparecchiature offerte siano state prodotte in regime di qualità, certificato ISO - 9001:2000 in corso di validità alla data di pubblicazione e di chiusura del Bando di Gara relativo alle apparecchiature in oggetto.
Il mantenimento della validità della certificazione viene richiesto anche per tutto l'arco della durata della manutenzione.
Dovrà essere prodotta tutta la documentazione (anche in autocertificazione) attestante la sussistenza di tutti i suddetti requisiti.

Dovrà inoltre essere prodotta tutta la certificazione (o autocertificazione) circa la sussistenza dei suddetti requisiti per le apparecchiature fornite.

8 REQUISITI DI CONFORMITÀ DELL'INFRASTRUTTURA

Dovranno essere rispettate tutte le disposizioni attualmente vigenti in materia di sicurezza dell'informazione, di privacy, emissioni elettromagnetiche, sia a livello nazionale che comunitario (o, in sua assenza, internazionale). A titolo puramente indicativo e non esaustivo, si riportano di seguito alcuni esempi:

- requisiti indicati dal D.Lgs. 19 settembre 1994 n.626;
- D.Lgs. 9 aprile 2008 n. 81 in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
- requisiti di ergonomia riportati nella direttiva CEE 90/270 recepita dalla legislazione italiana nella legge N.142 del 19 febbraio 1992;
- requisiti di sicurezza I.M.Q. (Istituto Marchio di Qualità) e di emissione elettromagnetica FCC (Federal Communications Commission); in alternativa, dovranno almeno rispettare analoghi requisiti certificati da altri Enti riconosciuti a livello europeo, nel qual caso l'Impresa dovrà allegare una descrizione delle prove effettuate e dei risultati ottenuti;
- Legge quadro 22 febbraio 2001, n. 36 "sulla protezione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici"
- norme di sicurezza CEI 74/2 (EN 60950/IEC 950);
- norme di sicurezza CEI 110/5 (EN 55022/CISPR 22);
- cablaggio strutturato EN 50173 e ISO/IEC 11801;
- misure dei parametri elettrici e trasmissivi secondo la norma IEC 1156;
- guaine secondo norme IEC 332-3 C.