ALLEGATO 4 - CAPITOLATO TECNICO

Gara per l'affidamento dei servizi di gestione in hosting del sistema informativo Consip – ID 1483

INDICE

1. PREMESSA

Il presente capitolato ha lo scopo di definire i requisiti relativi alla fornitura dei servizi in oggetto, in quantità, qualità e livelli di servizio adeguati allo sviluppo, alla manutenzione e all'hosting dei sistemi informativi di Consip S.p.A.

Con il termine "Consip" va intesa la CONSIP S.p.A.. Con il termine "Fornitore" va intesa l'Impresa aggiudicataria della fornitura.

Quando non diversamente specificato, con "capitolato" si intende il presente documento, con "gara" si intende la gara da effettuare a fronte del capitolato, con "contratto" si intende il contratto che verrà sottoscritto a seguito dell'aggiudicazione della gara, con "fornitura" si intende il complesso delle attività e dei prodotti che il Fornitore è chiamato a compiere e a produrre per onorare il contratto.

In genere, ogni altro termine che potrebbe essere scritto in minuscolo, viene scritto in maiuscolo quando assume un ben preciso significato ai fini della comprensione del testo (es. "analisi", per un'accezione qualsiasi presente in un dizionario della lingua italiana, "Analisi" ad indicare una ben precisa fase del ciclo di vita del software, specificatamente definita nel documento, ed il cui significato è formalmente collegato alla presente fornitura).

Nel capitolo 2 è descritto il contesto in termini di caratteristiche applicative e di ambienti tecnologici. L'oggetto della fornitura è riportato nel capitolo 3, con lo scopo di definire i servizi richiesti. Nel capitolo 4 sono analizzati i requisiti della fornitura, nonché i parametri quantitativi e le figure professionali (meglio approfondite in Appendice 2) previste per la fornitura. Le modalità di esecuzione dei servizi e delle attività nonché gli aspetti qualitativi della fornitura sono descritti nel capitolo 5.

Le prescrizioni contenute nel presente capitolato tecnico, ivi incluse le appendici sotto richiamate, rappresentano i requisiti minimi della fornitura.

La fornitura è articolata in un unico lotto.

Sono parti integranti del capitolato le seguenti appendici:

- Appendice 1: Livelli di Servizio (SLA);
- Appendice 2: Figure professionali per l'erogazione della fornitura;
- Appendice 3: Piano della sicurezza del Data Center;
- Appendice 4: Applicativi Consip.

All'atto della stipula del contratto sarà resa disponibile la documentazione relativa a standard dei documenti e all'utilizzo degli strumenti Consip a supporto della fornitura.

1.1 Termini, definizioni ed acronimi

Committente: si intende la Consip S.p.A.;

Consip: si intende la Consip S.p.A.;

Fornitore/Impresa/Aggiudicatario: si intende l'impresa o il RTI Fornitrice aggiudicataria della gara;

Fornitura: l'insieme dei prodotti software, hardware, dei servizi e di tutto ciò che è richiesto nel presente capitolato tecnico;

CS: Centro Servizi del Fornitore

Capitolato: si intende il presente documento;

Applicazione: una qualsiasi realizzazione software (ad-hoc o prodotto di mercato) tesa a fornire un insieme di funzionalità all'Amministrazione. Solitamente una applicazione è composta da uno o più moduli software e da un database a cui l'applicazione fa riferimento;

Servizi professionali**:** per servizi professionali si intendono : gestione applicativa, supporto specialistico, servizio di assistenza da remoto se richiesto;

VMware: società VMware Italy S.r.l.;

ELA: Enterprise License Agreement;

OdF: si intende "oggetto di fornitura", elemento hardware, prodotto software o servizio di manutenzione e supporto specialistico richiesto nel presente capitolato tecnico;

SLA: si intende Service Level Agreement, il livello di servizio;

LdS: si intende Livello di Servizio

Obiettivo: unità organica di lavoro in cui si scompongono i servizi erogati in modalità progettuale. Dal punto di vista del Fornitore l'obiettivo è assimilabile ad un "progetto", la cui esecuzione è suddivisa nelle fasi, indicate dal ciclo di vita applicato, che richiedono la realizzazione di specifici prodotti;

Front End: è un termine largamente utilizzato per caratterizzare le interfacce che hanno come destinatario un utente. Una applicazione front è un programma con il quale l'utente interagisce direttamente. In una applicazione web identifica le macchine su cui è installato il web server

Back end: è un termine largamente utilizzato per caratterizzare le interfacce che hanno come destinatario un programma. Una applicazione back end è un programma con il quale l'utente interagisce indirettamente, in generale attraverso l'utilizzo di una applicazione front-end. In applicazioni web multilivello identifica il data server: cioè il server in cui è installata la base dati

Load balancing: metodo con il quale le richieste di connessione ad un sito web vengono deviate fra server diversi che mantengono lo stesso sito.

Cluster: un insieme di macchine connesse tramite una rete telematica. Lo scopo di un cluster è quello di distribuire una elaborazione molto complessa tra i vari computer componenti il cluster. Le macchine suddividono i processi di un job su più macchine, al fine di guadagnare in prestazioni.

Web: Il World Wide Web in sigla WWW, comunemente abbreviato in Web è uno dei servizi di Internet, la più grande rete di computer mondiale e ad accesso pubblico esistente.

Browser web: programma che consente agli utenti di visualizzare e interagire con testi, immagini e altre informazioni, tipicamente contenute in una pagina web di un sito. Il browser è in grado di interpretare il codice HTML e visualizzarlo in forma di ipertesto.

P&C: Servizio Consip Pianificazione e Commesse

SIGeF: Sistema Informativo Gare e Fornitori

SIPAI: Sistema per la Pianificazione delle Attività IT

SIC: Sistema Informativo Consip;

ERP: Enterprise resource planning (letteralmente "pianificazione delle risorse d'impresa", spesso abbreviato in ERP) è un sistema di gestione, chiamato in informatica sistema informativo, che integra tutti i processi di business rilevanti di un'azienda (vendite, acquisti, gestione magazzino, contabilità etc.)

SFTP: L'SSH File Transfer Protocol o SFTP è un protocollo di rete che prevede il trasferimento dei dati e funzionalità di manipolazione. È tipicamente usato con il protocollo SSH-2 che utilizza un trasferimento dei file sicuro, anche se è utilizzabile con un qualsiasi altro protocollo.

FTP: Il File Transfer Protocol (FTP) (protocollo di trasferimento file), è un Protocollo per la trasmissione di dati tra host basato su TCP.

TWS: Acronimo di Tivoli Workload Scheduler

SSO: la capacità di un utente di autenticare una volta ed accedere a varie risorse di applicazione web che avrebbero richiesto altrimenti la singola autenticazione, con ogni autenticazione potenzialmente che richiede l'insieme differente delle credenziali.

2. Contesto della Fornitura

La necessità di una fornitura di servizi di hosting e gestione, nasce dal nuovo assetto della Consip dopo la scissione avvenuta il 1 luglio 2013. Attualmente il Sistema Informativo Consip è ospitato sulle infrastrutture, del Ministero dell'Economia e delle Finanze e dislocato in varie sedi.

A completamento della procedura di scissione, il Sistema Informativo Consip dovrà essere completamente separato dalla rete e dai servizi offerti dal MEF.

Questa riorganizzazione prevede che tutte le componenti IT, oggetto della presente fornitura, siano orientate verso outsourcing completo di servizi e che l'unità "Standard Sicurezza Sistemi Informativi Interni" avrà il governo della fornitura, mantenendo il possesso delle applicazioni e dati migrati in un ambiente presso il Centro Servizi (CS).

2.1 Oggetto della fornitura e dimensioni massime dei servizi

La Fornitura prevede l'erogazione dei seguenti servizi:

a) Servizi di connettività, quali:
   1. Consip-Centro Servizi (cfr. § 3.1.1);
   2. Centro Servizi-Internet (cfr. § 3.1.2);
   3. Consip-Internet (cfr. § 3.1.3);

b) Servizi di Hosting di:
   1. Server midrange (cfr. § 3.2.1 e § 4.2.1);
   2. Server entry-level (cfr. § 3.2.1 e § 4.2.1);
   3. SAN (Storage Area Network) (cfr. § 3.2.2.8);
   4. Protocollo informatico (cfr. § 3.2.2.1 e § 4.2.2.1);
   5. Conservazione sostitutiva (cfr. § 3.2.2.2 e § 4.2.2.2);
   6. Web (cfr. § 3.2.3 e § 4.2.3);

c) Servizi di Gestione di:
   1. Postazioni di Lavoro e apparati (cfr. § 3.3.2, §3.4 e § 4.3.2);
   2. Server(cfr. § 3.3.1 e § 4.3.1);

d) Servizi di Supporto Specialistico per:
   1. Attività di migrazione (cfr. § 3.5.1);

2. Consulenza (cfr. § 3.5.2).

Per quanto riguarda la gestione e consulenza il fornitore dovrà fornire appropriate figure professionali che siano in grado di svolgere le attività affidate.

Si precisa che la presente fornitura verrà erogata solo in ragione e nelle quantità richieste ed attivate dalla Consip sulla base di specifiche richieste.

Si rende noto, quindi, che i servizi oggetto della fornitura potranno essere non attivati, ovvero attivati solo parzialmente, ovvero disattivati in corso di esecuzione, e comunque, anche per tutta la durata contrattuale, richiedendo dimensioni inferiori alle dimensioni massime indicate nel presente capitolato.

Sulla base delle stime effettuate, si rende noto che, dal momento della stipula del contratto, i servizi verranno attivati secondo le dimensioni indicate nel presente capitolato, fermo restando che tutti i servizi, o parte di essi, ovvero anche uno solo di essi, potranno subire variazioni in aumento o in diminuzione, sempre nel limite delle dimensioni massime previste per ogni singolo servizio.

I servizi verranno attivati solo su richiesta della Consip fermo restando che è garantito al fornitore il 10% del corrispettivo massimo complessivo.

2.2 Durata della Fornitura

Il contratto avrà la durata di 36 mesi decorrenti dalla data di inizio fornitura. Si precisa che negli ultimi 3 mesi di efficacia del contratto dovranno essere erogate anche le attività di affiancamento verso un nuovo fornitore di servizi come descritto al successivo paragrafo 5.8.

3. GENERALITÀ DELLA FORNITURA

In questo capitolo verranno descritti tutti i servizi che saranno oggetto della fornitura. Si fa notare che, vista l'attuale struttura, la componente IT della Consip è dimensionalmente da assimilarsi a quella di una piccola o media impresa.

Per un approfondimento dei requisiti relativi ai servizi descritti nei seguenti paragrafi si rimanda al capitolo 4 "Requisiti della Fornitura".

3.1 Servizi di Connettività

Con la presente fornitura si richiede al Fornitore di realizzare un servizio di rete per interconnettere la sede Consip con il CS. Il CS esporrà in una intranet servizi che saranno raggiungibili da tutti gli utenti dotati di PdL situata nella sede Consip e da tutti coloro che, interconnessi con postazioni remote, abbiano attivato una connessione VPN.

Il Fornitore deve erogare il servizio di trasporto IP attraverso l'impiego di un idoneo apparato di accesso che metta a disposizione del cliente la banda richiesta.

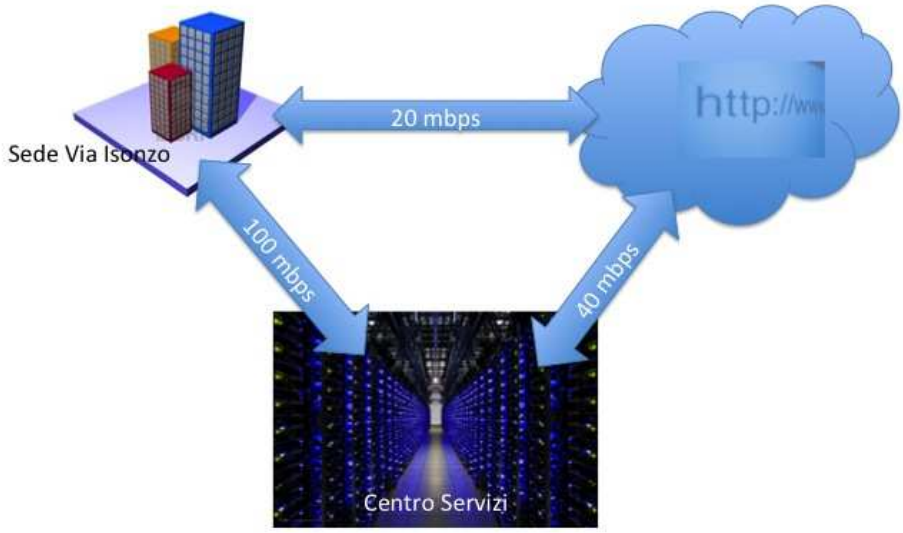
Il fornitore deve provvedere:

- ad installare e configurare tutti gli apparati di Terminazione di Rete (Router) presso la sede della Consip per la connessione al CS (i TdR dovranno essere dotati di almeno 24 porte LAN);
- ad amministrare tali apparati coordinandosi con Consip.

Per le connessioni della sede Consip al CS è richiesto un servizio ad alta affidabilità. Per questo motivo il fornitore dovrà mettere a disposizione, presso la sede, l'accesso secondario su un differente TdR.

I TdR dovranno essere allo stato dell'arte della tecnologia e del mercato, dovranno implementare protocolli allo stato dell'arte e dovranno essere dimensionati in modo da garantire il rispetto dei livelli di servizio previsti per il servizio di trasporto richiesto.

Di seguito uno schema di massima dell'infrastruttura di rete dove i collegamenti di rete al centro servizi dovranno essere ridondati.



La fornitura di connettività dovrà consentire la connessione al Centro Servizi della sede di Consip di via Isonzo 19 con banda massima di accesso di 150 mbps garantita all'80%, una connessione dal Centro Servizi verso Internet con banda massima di accesso di 60 mbps garantita all'80%, e di una connessione direttamente esposta su Internet con banda massima di accesso di 30 mbps garantita al 50%. Tale infrastruttura di rete dovrà essere facilmente scalabile per supportare eventuali nuove esigenze di Consip.

Si stima che, al momento della stipula, verrà attivato il servizio di connettività con le seguenti dimensioni:

- Consip - Centro servizi: banda massima di accesso di 100 mbps garantita all'80%;
- Centro Servizi – Internet: banda massima di accesso di 60 mbps garantita all'80%;
- Consip – Internet: banda massima di accesso di 20 mbps garantita al 50%.

3.1.1 Connettività Consip – Centro Servizi

Il Fornitore dovrà erogare un servizio con Banda Massima in Accesso, che al momento della stipula si stima che verrà attivata a 100 mbps, con valori uguali per la direzione Upstream (BMAu) e la direzione Downstream (BMAd).

Il Fornitore deve assicurare, attraverso opportune misure tecnico-organizzative (ad es. ridondanza dell'infrastruttura fisica di accesso, back-up, ridondanza degli apparati di accesso, presidi tecnici presso il cliente) il rispetto dei valori di disponibilità dell'accesso, tempo di ripristino, ripetitività dei disservizi e finestra temporale di erogazione secondo i livelli di servizio che verranno definiti nel presente Capitolato e nelle sue appendici.

I servizi di connettività dovranno essere caratterizzati almeno da una disponibilità ≥ 99,95% e si richiede la fornitura di linee di backup tramite la fornitura di accesso secondario con BMA pari almeno alla metà di quella principale con un TdR dedicato.

Il Fornitore deve mettere a disposizione una rete ridondata in fibra ottica a doppio instradamento.

Per quanto riguarda la Qualità del servizio dovrà essere possibile gestire policy di Quality of Service tali per cui l'allocazione della banda su alcuni protocolli o servizi sia garantita con livelli definiti in Appendice 1 "Livelli di servizio".

3.1.2 Connettività Centro Servizi Internet

Il Fornitore dovrà erogare un servizio con Banda Massima in Accesso, che al momento della stipula si stima che verrà attivata a 40 mbps, con valori uguali per la direzione Upstream (BMAu) e la direzione Downstream (BMAd) in modo da connettere il centro servizi alla rete Internet attraverso opportuni apparati di sicurezza. Tale connettività verrà utilizzata dagli utenti Consip per raggiungere la rete Internet.

I servizi di connettività verso Internet dovranno essere caratterizzati almeno da una disponibilità pari al ≥ 99,9%.

3.1.3 Connettività Consip – Internet

Il Fornitore deve predisporre un servizio di connettività dedicato al collegamento diretto ad Internet che sia indipendente dal Centro Servizi allo scopo di consentire la sola navigazione alla rete di fornitori o di eventuali ospiti presenti nella sede Consip, con Banda Massima in Accesso, che al momento della stipula si stima che verrà attivata a 20 mbps.

I servizi di connettività dovranno essere caratterizzati almeno da una disponibilità unitaria del 98%, senza necessità di una linea di backup.

La connettività verrà erogata in modalità wired e in modalità wireless attraverso la rete wireless di proprietà della Consip.

3.2 Servizi erogati tramite il Centro servizi

Il CS, ospitato presso i Data Center messi a disposizione dal Fornitore, sarà il punto di accesso centralizzato per gli applicativi sviluppati e utilizzati da Consip, avrà funzione di Security Operation Center (SOC), Data Center Storage e di Internet Access Point (IAP).

Il Fornitore dovrà prevedere un architettura ridondata dei suoi Data Center per consentire la distribuzione del carico e la tolleranza ai guasti. I Data Center dovranno essere conformi ai principali standard di sicurezza internazionali e implementare un Sistema di Gestione della Sicurezza delle Informazioni Certificato secondo lo standard internazionale ISO IEC 27001.

Il Centro Servizi dovrà mettere a disposizione di Consip sia server fisici sia server virtuali adatti ad ospitare tutti i servizi che verranno descritti nei capitoli successivi. Il Fornitore

dovrà configurare, in accordo con Consip, sufficienti apparati che consentano di distribuire il carico di elaborazione di uno specifico servizio tra più server (Load Balancing), in modo da poter rispettare le specifiche funzionali dei livelli di servizio e di QoS.

3.2.1Servizi di Hosting

Il Fornitore dovrà nominare al suo interno un **Responsabile operativo dei servizi di hosting** che dovrà fungere da punto di contatto prioritario per tutte le problematiche inerenti agli ambienti e alle applicazioni ospitate nel proprio Data Center. Il Fornitore metterà a disposizione e configurerà gli apparati nel Centro Servizi in modo che possano ospitare gli applicativi utilizzati dalla rete Consip, attualmente su infrastruttura di proprietà del MEF.

Il Fornitore quindi dovrà mettere in essere tutte le attività per creare le condizioni operative per poter migrare le applicazioni Consip verso il proprio CS.

Il porting delle applicazioni Consip verso il Data Center del Fornitore dovrà, per quanto possibile, far uso di server virtuali allo scopo di consentire una maggiore flessibilità dell'infrastruttura e sua scalabilità nel tempo.

Per maggiore dettaglio e per consentire al Fornitore di comprendere l'attuale contesto tecnologico (come ad esempio i sistemi di bilanciamento del carico eventualmente necessari all'erogazione dei servizi) degli applicativi utilizzati da Consip verranno descritti i Sistemi da sottoporre a migrazione all'interno dell'Appendice 4. Per quanto riguarda le componenti software (SO, Webserver, Application Server, Software Proprietari, ecc.) che verranno descritte in tale appendice, la valorizzazione delle versioni è puramente indicativa e potrà essere oggetto di variazioni nei periodi antecedenti il porting verso il Fornitore e anche successivamente nel corso della fornitura.

I Servizi di Hosting che dovranno essere erogati dal Fornitore possono essere assimilabili a quelli definibili come IAAS (Infrastructure As A Service) dove viene richiesta principalmente la virtualizzazione di una infrastruttura. Sarà onere del Fornitore mettere a disposizione, per tutta la durata del contratto, una infrastruttura in grado di ospitare tutte le applicazioni di volta in volta sviluppate e o modificate da Consip, ferme restando le dimensione massime indicate al capitolo 4.2.1.

Il Fornitore dovrà farsi carico di tutte le problematiche di gestione sistemistica per gli ambienti messi a disposizione, come ad esempio i sistemi operativi o la gestione del bilanciamento del carico.

Si rende noto al Fornitore che, con l'esclusione dei Sistemi Operativi, le licenze d'uso per i software e le relative licenze di manutenzione saranno a carico di Consip.

Tutti i requisiti per la realizzazione dei servizi che il fornitore dovrà erogare, sono riportati al capitolo 4.

3.2.1.1 *Servizi hosting di aree di Collaudo e Test*

La fornitura di hosting di servizi dovrà consentire la replica degli ambienti su server (anche virtuali) separati da quelli dove sono ospitate le applicazioni in esercizio. Il Fornitore quindi dovrà predisporre sufficienti apparati per poter creare un area di collaudo e test. Quest'area sarà utilizzata da Consip, ovvero da terze parti delegate per lo sviluppo/aggiornamento degli applicativi Consip.

3.2.1.2 *Backup e Restore ambiente hosting*

Per il servizio di Backup & Restore il Fornitore dovrà fare copia e salvare i dati e le configurazioni operative sia degli ambienti server mediante l'utilizzo di supporti esterni conservati in locali diversi da quelli delle apparecchiature. Questa conservazione dovrà consentire il ripristino dei contenuti/applicativi/configurazioni in caso di indisponibilità/danneggiamento degli ambienti operativi.

Per quanto riguarda il sistema di Backup & Restore del CS il Fornitore dovrà fornire la documentazione a supporto delle policy di backup previste nel Centro Servizi dove verranno definiti anche i tempi di ripristino dopo una apertura di un ticket di assistenza.

Le politiche di backup da applicare ai vari ambienti in esercizio saranno da concordare con Consip in fase di definizione del Piano di Migrazione e dovranno essere attuate alla presa in gestione delle infrastrutture che ospitano le varie applicazioni di Consip.

3.2.2Servizi totalmente Esternalizzati

In questo capitolo sono descritti i servizi per i quali Consip non richiede specifici requisiti architetturali (Hardware, Software, SO ecc.), ma solo specifiche funzionali del servizio e suoi SLA.

3.2.2.1 *Protocollo informatico*

Il Fornitore dovrà fornire un servizio di protocollazione informatizzata che rispetti le direttive contenute nel Codice dell'Amministrazione Digitale modificato dal decreto legge 21 giugno 2013 n. 69, convertito con modificazioni dalla L. 9 agosto 2013, n. 98 in materia di segnatura di protocollo informatico e gestione documentale.

La soluzione di protocollo informatico individuata dovrà fornire i servizi di:

- protocollazione e classificazione dei documenti che verranno forniti in formato PDF (Portable Document Format);
- completamento della protocollazione sulla base di uno schema di classificazione con riferimento agli atti con dati in tutto o in parte mancanti;

Il Fornitore dovrà mettere a disposizione un sistema di ricerca della documentazione che consenta l'estrazione del documento in base a campi predefiniti (numero protocollo, anno, tipo di documento ecc.).

3.2.2.2 *Conservazione sostitutiva*

Il Fornitore dovrà fornire il servizio di Conservazione Sostitutiva in accordo con le regole tecniche di cui alla Circolare Cnipa n. 11/2004 "*Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.*".

Tale servizio consentirà la conservazione in formato elettronico a norma dei documenti di Consip .

Il Fornitore individuerà un "**Responsabile del servizio di Conservazione**", che dovrà garantire gli standard di sicurezza, l'adeguamento delle risorse tecnologiche messe a disposizione dal Fornitore, nonché il costante allineamento del sistema alle evoluzioni della normativa;

La Conservazione Sostitutiva dovrà consentire almeno:

- Raggruppamento dei documenti in lotti da avviare alla conservazione;
- Apposizione della marcatura temporale e la firma digitale su singoli o su interi lotti inseriti in conservazione;
- Restituzione al cliente di un archivio contenente gli identificativi dei documenti;
- Possibilità, da parte di Consip, di effettuare ricerche dei documenti in tempo reale, anche a seguito di controlli da parte di terzi direttamente accedendo al sistema ospitato nel CS ovvero su eventuali supporti di consultazione prodotti periodicamente dal Fornitore, o di ricevere i documenti via e-mail;
- Produzione e successiva estrazione delle impronte dei documenti storicizzati;
- Realizzazione di tutti gli altri servizi per l'adempimento delle normative in vigore in tema di conservazione sostitutiva;
- Garanzia di leggibilità nel tempo dei documenti conservati;
- Garanzia sia informatica sia fisica della sicurezza della base dati, provvedendo ad adottare gli standard stabiliti dalla legge;
- Garanzia, nel tempo, dell'integrità dei documenti contenuti nei supporti di memorizzazione anche attraverso il loro riversamento su supporti di nuova generazione;
- Garanzia del rispetto dei termini previsti per la conservazione delle tipologie documentali, quando la normativa lo prevede.

3.2.2.3 *File server*

Viene richiesto al Fornitore di predisporre i sistemi per erogare il servizio di File Server all'interno della propria infrastruttura ospitata nel CS.

Si richiede al Fornitore di garantire le seguenti attività:

- creazione di Share di rete;

- ampliamento di Share di rete;
- restore di file da una share di rete;
- gestione Distributed File System (DFS);
- esecuzione periodica dei backup dei file server;
- manutenzione periodica dei file server (installazione patch raccomandate, upgrade moduli software, ...);
- monitoraggio delle performance del file server, dello spazio disponibile sul file server, prevenzione della saturazione dei file system;
- attribuzione e revoca dei diritti di accesso alle share di rete.

3.2.2.4 *Active Directory*

Il Fornitore dovrà prevedere nella sua architettura l'installazione e configurazione di un Active Directory (AD) che sarà copia dell'AD di proprietà Consip, installato nella sede di via Isonzo, 19.

3.2.2.5 *DNS*

Il Fornitore dovrà rendere disponibile un servizio di DNS per lo spazio dei nomi interni alla intranet Consip.

Il Fornitore dovrà assicurare la continuità del servizio DNS prevedendo adeguati meccanismi di "backup a caldo".

Il Fornitore dovrà erogare il servizio di DNS primario per la risoluzione dei nomi Internet esterni a Consip, DNS secondario, DNS Reverse.

3.2.2.6 *Fax Server*

Il Fornitore dovrà predisporre un servizio che consenta l'invio/ricezione di documenti fax utilizzando interfacce comuni. Il servizio dovrà consentire di:

- Inviare e ricevere Fax via Email dal PC o dal cellulare;
- Archiviare e Protocollare i Fax in digitale in formato PDF;
- Ricercare qualsiasi Fax ricevuto e spedito;
- Stampare i Fax;
- Inviare lo stesso Fax contemporaneamente a più utenti;

3.2.2.7 *Proxy Server*

Tutti gli utenti Consip, circa 350 utenze, devono poter accedere ad Internet attraverso opportuni apparati proxy allo scopo di migliorare le performance del sistema, filtrare le richieste di accesso a determinati siti web. Il Fornitore dovrà quindi mettere a disposizione nel suo il CS un servizio proxy che non introduca latenze.

Il Fornitore dovrà prendersi carico delle seguenti attività:

- Gestione della disponibilità e delle performance dei servizi web in accordo con gli SLA indicati nell'Appendice 1;
- Configurazione e monitoraggio dei proxy server;
- Modifiche delle configurazioni su specifiche richieste di Consip.

3.2.2.8 *SAN*

Il Fornitore dovrà mettere a disposizione una Storage Area Network (SAN) ad alta velocità di trasmissione e affidabilità costituita esclusivamente da dispositivi di memorizzazione di massa, con protocolli FC (Fiber Channel) o iSCSI (Internet SCSI), allo scopo di rendere disponibili tali risorse di immagazzinamento (storage) alle applicazioni Consip.

La dimensione massima di questa area di storage dovrà essere di 20TByte con la possibilità di scalare verso l'alto in accordo con un listino nel quale siano definiti i costi/caratteristiche per l'ampiamento degli spazi di memorizzazione.

Si stima che, al momento della stipula, verrà attivato uno spazio disco SAN pari a 10 TByte.

3.2.2.9 *Backup & Restore dei Servizi esternalizzati*

Il Fornitore dovrà erogare un servizio di back-up/restore che garantisca a Consip il salvataggio dei dati presenti sui server. Tale servizio ad alto livello di sicurezza, garantirà il recupero dei dati, in caso di perdita dovuta a guasti hardware o malfunzionamenti del software, permettendone la ricostruzione ad una certa data.

In particolare si richiede al Fornitore di implementare una politica di backup in modo che sia possibile recuperare dal singolo item, fino all'intero set di informazioni gestite.

Il Fornitore dovrà concordare con Consip le politiche di backup e loro schedulazione.

3.2.3Servizi di Hosting esposti verso l'esterno

Le applicazioni e i servizi che saranno esposti su Internet dovranno essere ospitati in un opportuna area logica del CS. Di seguito riportiamo tali servizi.

3.2.3.1 *Servizi di Web Hosting*

Il Fornitore dovrà ospitare l'attuale portale web Consip, che sarà raggiungibile attraverso protocollo di comunicazione Http e il protocollo sicuro Https.

Il web server dovrà mettere a disposizione tutti gli applicativi/linguaggi di programmazione necessari per la pubblicazione del sito web (php5, asp, ruby, ISS/Apache, ecc.) che attualmente è sviluppato con tecnologie open (openCMS), ed uno spazio adeguato di archiviazione dei dati.

Il Fornitore dovrà gestire il dominio di 2° livello e consentire illimitati domini di 3° livello che potranno essere attivati in futuro.

L'amministrazione del sito web dovrà essere possibile attraverso una console o interfacce di controllo predisposti dal Fornitore. Per maggiori dettagli dell'architettura richiesta si rimanda allo specifico paragrafo dell'Appendice 4.

3.2.3.2 *Ftp e SFtp server*

Il Fornitore dovrà erogare il Servizio di FTP e FTP su SSH attraverso l'infrastruttura disponibile nel CS.

Il servizio di gestione dei server di FTP deve garantire il corretto funzionamento del trasferimento dei file di dati in maniera affidabile ed efficiente.

Si richiede al Fornitore di garantire la disponibilità e il corretto funzionamento dei server FTP, attraverso l'esecuzione di Attività Operative che includono:

- la configurazione e la gestione degli account e dei direttori di file transfer;
- l'applicazione delle policy di accesso;
- il controllo e monitoraggio delle attività da e verso l'FTP server

3.2.4Servizi di sicurezza logica

Il Fornitore deve nominare al suo interno un **Responsabile operativo locale della sicurezza** che dovrà fungere da punto di contatto prioritario per tutte le problematiche di sicurezza. Il Responsabile Operativo della sicurezza potrà avvalersi di sostituti i cui nominativi dovranno essere preventivamente comunicati a Consip. Il Fornitore dovrà predisporre un opportuno Piano della Sicurezza del Centro Servizi che dovrà contenere una descrizione approfondita sulle modalità logistiche ed organizzative, gli strumenti ed i sistemi che il Fornitore intende adottare o di cui è provvisto per rendere sicuro e protetto l'ambiente in cui sono ospitati le infrastrutture, il software e i dati informativi della Consip.

I contenuti del Piano della Sicurezza sono descritti nell'Appendice 3 – Piano della sicurezza del Centro Servizi. Tale piano diverrà parte integrante del Piano di Migrazione più avanti richiamato.

3.2.4.1 *Firewalling*

Il Fornitore dovrà implementare e gestire, mediante apparati hardware/software, un sistema di firewalling ridondato che permetta di analizzare il traffico che lo attraversa, bloccando i pacchetti di rete che appartengono a collegamenti non permessi secondo le regole di protezione configurate dal Fornitore sulla base delle esigenze espresse da Consip.

La selezione ed implementazione della tipologia di dispositivo di tipo firewall, stante i requisiti del presente capitolato tecnico, è a carico del Fornitore.

Il firewall dovrà essere configurato in modo che il flusso dati tra la rete interna Consip (intesa come l'insieme dei segmenti LAN protetti) e la rete del Fornitore transiti esclusivamente attraverso di esso.

3.2.4.2 *Network Intrusion Detection/Prevention System (NIPS & NIDS)*

Il Fornitore dovrà implementare e gestire un sistema di prevenzione e rilevamento delle intrusioni che consenta di rilevare tutte le sequenze di eventi condotti da una o più entità non autorizzate, aventi come obiettivo la compromissione di un sistema, di un apparato o della rete.

Il sistema dovrà prevedere meccanismi di notifica anche verso Consip a fronte dell'identificazione di un evento di attacco.

3.2.4.3 *VPN*

L'accesso alle risorse e applicativi offerti dal Centro Servizi dovrà essere consentito anche da postazioni remote permanenti o temporanee tramite VPN ad elevata sicurezza.

Il Fornitore dovrà predisporre specifici apparati (concentratori VPN) per consentire all'infrastruttura di rete una connessione remota SSL-VPN. Ciascun utente dovrà potersi connettere alla rete Consip con il proprio Browser Web collegandosi all'indirizzo IP pubblico fornendo le corrette credenziali d'accesso.

Gli utenti che si collegano tramite SSL-VPN devono poter essere gestiti in maniera personalizzata. A ciascun utente dovrà essere possibile assegnare un indirizzo IP statico, un gruppo predefinito e dei filtri per limitare l'accesso alle aree di lavoro. Inoltre dovrà essere possibile limitare la quantità di applicazioni (plug-in) che ciascun utente SSL-VPN potrà utilizzare.

Il Fornitore dovrà erogare anche un servizio di VPN basato sullo standard IPsec come definito dall'IPsec Working Group dell'IETF (RFC 2401).

I sistemi offerti dovranno realizzare i protocolli AH (Authentication Header) e ESP (Encapsulating Security Payload).

Il servizio erogato dal Fornitore dovrà prevedere il supporto per IPsec Tunnel Mode e Transport Mode.

Il Fornitore si impegna ad erogare il servizio VPN IPsec utilizzando certificati X.509v3 emessi esclusivamente da una propria Certification Authority di rete. Il formato per le richieste dei certificati dovrà essere conforme allo standard PKCS. Il servizio dovrà prevedere l'adozione di adeguati meccanismi di protezione della chiave privata e delle chiavi di sessione memorizzate nel dispositivo.

3.2.4.4 *Antivirus e Content Filtering*

Il Fornitore dovrà mettere a disposizione un servizio di Antivirus e Content Filtering Management che consiste nell'implementazione e nella gestione di un sistema di protezione del Sistema Informativo della Consip da spamming, da attacchi veicolati tramite il protocollo HTTP e da codice software eseguibile (Virus, Worm, Trojan, ecc.).

Il Fornitore dovrà garantire le seguenti caratteristiche del servizio:

- Antivirus Gateway (AVG): gestione di un sistema per la protezione da codice dannoso che può propagarsi tramite lo scambio di posta elettronica;
- HTTP Gateway (HTTPG): gestione di un sistema per la protezione da codice dannoso che può propagarsi per il tramite della navigazione web e per la protezione da attacchi informatici veicolati tramite il protocollo HTTP;
- FTP Gateway (FTPG): gestione di un sistema per la protezione da codice dannoso che può propagarsi per il tramite del trasferimento di file mediante FTP.

Il sistema di Antivirus dovrà garantire la rilevazione dei virus noti, recensiti e pubblicamente elencati dalle organizzazioni preposte, indipendentemente dalla piattaforma ospite e dal media di trasmissione ed inoltre dovrà essere in grado di effettuare delle scansioni sul traffico analizzato in modo da individuare anche virus non precedentemente noti.

Il servizio fornito dal Fornitore dovrà garantire la capacità di scansione in tempo reale, piena interoperabilità e/o trasparenza tra client e server.

Il servizio erogato dal Fornitore dovrà prevedere il supporto di file in formati compressi (zip, gzip, rar) per il controllo sulla presenza di codice dannoso.

Per quanto riguarda la caratteristica di AVG esso dovrà garantire almeno le seguenti ulteriori funzionalità:

- capacità di riparare file e/o messaggi infetti, nel caso di virus per i quali esiste la possibilità di recupero;
- capacità di eseguire la scansione differita di interi file/documenti allegati;
- supporto blacklist (liste contenenti domini di mail o indirizzi di mail indesiderati);
- configurazioni antispamming che consentano il blocco di messaggi di posta elettronica che transitano per il gateway basati su blacklist e riconoscimento di porzioni del contenuto del messaggio di posta elettronica personalizzabili;
- verifica sintattica e semantica sul header dei messaggi;
- Capacità di filtrare messaggi di phishing.

3.2.4.5 *Servizio Antivirus sui server erogati*

Il Fornitore deve prevedere che i server erogati dal servizio hosting siano dotati di Antivirus di classe enterprise in modo che sia possibile prevenire le eventuali infezioni causate da codice malevolo.

Il Fornitore deve provvedere a gestire in modo efficace le contromisure atte a contrastare la diffusione di virus o worm su sistemi server. Il servizio offerto dovrà prevedere anche la gestione sistemistica e la manutenzione dei componenti utilizzati.

3.2.5Servizi di sicurezza

Il Fornitore dovrà fare in modo che i suoi Data Center siano sicuri e protetti da accessi indesiderati e che consentano l'accesso a specifiche zone al solo personale autorizzato.

Il Fornitore dovrà utilizzare un registro elettronico interno delle visite in grado di gestire una blacklist dei visitatori cui non è consentito l'accesso ai locali.

I server dislocati presso il Data Center dovranno prevedere dei meccanismi di sicurezza fisica che impediscano il furto locale di dati (es. blocco di tutte le periferiche rimovibili scrivibili quali floppy, dispositivi USB, disabilitazione del boot da periferiche rimovibili).

Il Fornitore dovrà assicurare apparati di continuità dell'energia elettrica e utilizzare un sistema di segnalazione degli allarmi di tipo locale o remoto.

Le aree destinate ad ospitare gli apparati dovranno avere sistemi di climatizzazione appropriati, protette contro gli incendi e contro gli allagamenti mediante idonee misure di rilevazione ed intervento.

Nel caso i locali si trovino a livello stradale o inferiore, dovranno essere previsti sistemi anti-allagamento dotati di opportune pompe idrauliche.

Gli apparati attivi di rete dovranno essere compartimentati mediante armadi di cablaggio con chiusura a chiave.

3.2.5.1 *Disaster Recovery*

Il Fornitore dovrà apportare appropriate misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi richiesti, a fronte di gravi emergenze che ne intacchino la regolare attività.

Un piano d'emergenza deve prevedere il ripristino di tutte le funzioni richieste da Consip.

Il Fornitore dovrà quindi mettere a disposizione almeno un Data Center alternativo che si trovi localizzato sul territorio nazionale ad un opportuna distanza rispetto al Data Center primario e che abbia tutte le caratteristiche di sicurezza e capacità elaborativa per erogare tutti i servizi richiesti dal presente capitolato.

I Data Center dovranno essere tra di loro interconnessi con linee ad alta velocità ed efficienza tali da consentire un rapido ripristino dei servizi richiesti da Consip.

3.2.5.2 *Gestione degli Incidenti*

Il Fornitore dovrà, sotto richiesta di Consip, fornire i dati di log delle apparecchiature per consentire alle autorità competenti di poter indagare in modo appropriato sugli eventuali incidenti di sicurezza, di accesso non autorizzato alla documentazione riservata di Consip.

In particolare, per quanto riguarda la gestione degli incidenti di sicurezza, i requisiti sono:

- la procedura di contenimento deve essere preventivamente concordata, almeno nei contenuti generali;
- la notifica di un incidente o di un'anomalia di sicurezza deve avere SLA stringenti su base 24/7;
- in caso di incidente grave (codice rosso) deve essere attivato un contatto diretto con il responsabile della gestione dell'incidente lato fornitore;

- deve essere possibile ottenere copie forensi della memoria volatile delle macchine e dei dischi;
- deve essere possibile concordare la strategia e le attività di contenimento di un incidente;
- la strategia e le attività di contenimento devono essere attuate con SLA stringenti;
- in caso di incidente di sicurezza il rapporto con le forze dell'ordine deve essere gestito da Consip;
- in caso di incidente di sicurezza il rapporto con i media deve essere gestito da Consip;
- a chiusura di un incidente di sicurezza deve essere prodotto un rapporto di chiusura dell'incidente il cui indice dei contenuti deve essere concordato con Consip.

3.2.5.3 *Security host hardening*

Il Fornitore deve provvedere alla realizzazione, manutenzione e controllo delle politiche di hardening dei sistemi server (sistema operativo e applicazioni base) in modo tale da non comportare disservizi nelle ore in cui la sede Consip è attiva. Le politiche di hardening dei server dovranno essere concordate con Consip all'atto della stesura del Piano di Migrazione.

3.2.6Provisioning, Configuration e Change Management

Il Fornitore dovrà farsi carico di tutte le attività di installazione/configurazione e aggiornamento del software sugli apparati utilizzati per l'erogazione dei servizi.

Il Fornitore dovrà aggiornare il software degli apparati utilizzati per mantenere l'allineamento con i rilasci software messi a disposizione dai fornitori della tecnologia sia con finalità di patching che per quanto riguarda l'introduzione dei nuovi servizi.

Il Fornitore, su richiesta di Consip, dovrà apportare le modifiche sulle configurazioni dei server e del middleware, compatibilmente con gli SLA definiti nell'Appendice 1.

Il Fornitore dovrà effettuare eventuali variazioni delle componenti dei servizi erogati e delle configurazioni di rete e di sicurezza adottate.

Il Fornitore dovrà provvedere all'attuazione degli adeguamenti e/o riconfigurazioni richieste da attività di "system tuning".

A valle dell'installazione e configurazione, il Fornitore dovrà redigere e consegnare a Consip un inventario degli apparati, fisici o virtuali, installati e aggiornare puntualmente tale documento ogni volta si verifichi una modifica dello stato, sia software che Hardware.

3.3 Servizio di Assistenza

Il Fornitore dovrà fornire un servizio differenziato di assistenza:

- **Service Desk:** servizio volto alla risoluzione della problematiche inerenti alla connettività e ai servizi erogati dal Centro Servizi (Hosting, Posta elettronica, Servizi VPN, ecc..);

- **Help Desk:** il servizio volto alla risoluzione di malfunzionamenti delle postazioni di lavoro, e della gestione e configurazione degli apparati di rete presenti in Consip (hotspot Wi-Fi, Patch rete, Switch, ecc.).

3.3.1 Service Desk

Al fine di garantire il corretto funzionamento dei servizi di connettività e dei servizi erogati dal Centro Servizi, il Fornitore dovrà predisporre all'interno della sua organizzazione un servizio di Service Desk che avrà funzione di unico punto di contatto per la risoluzione di problematiche di questa tipologia.

Il Service Desk dovrà ricevere segnalazioni di malfunzionamento/anomalia sia tramite un sistema di Trouble Ticketing che attraverso chiamata telefonica/e-mail.

Il Fornitore deve impegnarsi all'apertura proattiva di un ticket sul TTS anche in mancanza di segnalazioni da parte di terzi, in risposta a malfunzionamenti rilevati dai propri sistemi di gestione. Il Fornitore è responsabile della gestione di tutti i casi in cui sia rilevabile un'interruzione o un degrado nella fruizione del servizio da parte dell'utente finale.

Il servizio di Service Desk dovrà garantire almeno le seguenti attività secondo gli SLA indicati in Appendice 1:

- installazione, attivazione, cessazione e variazione dei servizi e delle relative componenti;
- supervisione della rete e gestione degli apparati;
- mantenimento delle misure di sicurezza minime sulle infrastrutture utilizzate per i servizi di connettività;
- supporto tecnico alla gestione dei malfunzionamenti;
- gestione centralizzata delle configurazioni e distribuzione del software di rete;
- analisi delle prestazioni del servizio;

Il Service Desk dovrà fornire assistenza anche alle problematiche segnalate dagli utenti Consip per i servizi PEL e PEC e quindi dovrà garantire almeno le seguenti attività:

- eseguire il reset delle password delle utenze di accesso alle caselle;
- eseguire le richieste di "change" riguardanti modifiche sull'anagrafica degli utenti presenti sulla rubrica, sugli attributi delle caselle e sulle liste di distribuzione;
- eseguire le richieste di "change" riguardanti la creazione, cancellazione, blocco delle caselle e delle liste di distribuzione;
- coinvolge, se necessario, l'assistenza on-site (Help Desk);
- documentare i livelli di servizio dell'intero servizio.

3.3.2 Help Desk

Il Fornitore dovrà predisporre un servizio di assistenza per le PdL da remoto e dislocare del personale tecnico presso la Consip allo scopo compiere tutte le attività non risolvibili in modalità remota sulle PdL e le attività di gestione degli apparati (AD, Sistema di Backup, apparati di rete wireless e wired ecc.) presenti nella sede Consip.

Si stima che per erogare questo servizio nel rispetto degli SLA definiti in Appendice 1, sia necessaria la presenza di due FTE (Full Time Equivalent) qualificati a svolgere le attività descritte.

Le risorse impegnate, oltre a possedere le specifiche competenze tecniche, dovranno avere capacità nel distinguere tra problemi sporadici e problemi ricorsivi, attivandosi di conseguenza al fine di garantire la massima soddisfazione dell'utente.

Il servizio di assistenza è rivolto a due tipologie di utenze con diverse modalità di intervento:

- **per gli utenti VIP** (Circa 50 utenti) – attraverso interventi presso la postazione di lavoro dell'utente;
- **per gli utenti standard** - attraverso il controllo da remoto, utilizzando gli strumenti che saranno resi disponibili dal Fornitore. Nel caso in cui l'intervento così effettuato non sia sufficiente al ripristino della piena funzionalità delle PdL, è richiesto che l'operatore si rechi presso la postazione dell'utente.

Nel caso di indisponibilità espressa dall'utente ad un intervento on site, il personale del Fornitore provvederà a concordare un intervento presso la PdL su appuntamento (data/ora); in tal caso il livello di servizio decorrerà a partire dalla data/ora concordata.

A titolo esemplificativo e non esaustivo, si elencano le attività che dovranno essere effettuate:

- risoluzione dei problemi di funzionalità delle apparecchiature Consip affidate in gestione, anche in relazione alle connessioni di rete, ai punti rete e agli apparati di rete (attivi e passivi);
- risoluzione dei problemi segnalati dagli utenti dovuti a malfunzionamenti riconducibili alle PdL;
- laddove necessario e/o richiesto, salvataggio e ripristino dei dati;
- attivazione, supervisione e governo degli interventi di fornitori terzi (hw/sw/applicativi) e, unitamente agli stessi, verifica della piena funzionalità a seguito dell'intervento;
- riconfigurazione delle apparecchiature a seguito di interventi di ripristino delle funzionalità, anche se effettuati da fornitori terzi;
- supporto telefonico e/o tramite l'uso di software di management remoto, agli utenti e/o agli altri gruppi di supporto;
- supporto ad utenti nell'utilizzo di applicativi client standard (Office, Mail, Web Browser, ecc.) nonché nell'utilizzo delle Unità mobili aziendali (Blackberry, Smartphones, Palmari).

3.3.2.1 *Servizio gestione e manutenzione per le PdL*

Il numero delle PdL di Consip è stimato in circa 400 unità, mentre le utenze sono un sotto insieme di quest'ultime. L'obiettivo del servizio è quello di gestire in maniera efficace, proattiva e completa le PdL e i punti rete nella sede Consip, al fine di mantenerli in perfetta efficienza.

Il servizio di gestione PdL, dovrà essere erogato, oltre ai PC/notebook aziendali, anche per le periferiche (stampanti, scanner, ecc.), nonché per telefoni cellulari, Blackberry, IPAD, Tablet e palmari, ecc.

Il Servizio di gestione delle PdL dovrà prevedere anche le attività IMAC, ovvero le attività di installazione, movimentazione, aggiunta e cambiamento sulle postazioni lavoro.

Potrà essere richiesta, per alcune classi di utenti, la configurazione e l'installazione di prodotti sw specifici.

A titolo esemplificativo e non esaustivo, si elencano le attività che dovranno essere effettuate:

- attività propedeutiche per l'attivazione di nuove PdL, comprendendo la supervisione delle attività di fornitori terzi nella consegna ed installazione di nuove apparecchiature e del software;
- installazione, configurazione, personalizzazione e modifica delle apparecchiature, comprendendo il collegamento alla rete elettrica e dati e la configurazione delle utenze di accesso, ai servizi di rete ed alla posta elettronica nonché, laddove necessario, il salvataggio e il ripristino dei dati dell'utente;
- installazione ed aggiornamento delle componenti Sw di base (compresa la migrazione del Sistema Operativo), antivirus, componenti applicative e di produttività individuale standard e specifiche, anche attraverso attività di software distribution;
- installazione sulle PdL, di componenti hardware aggiuntive;
- manutenzione preventiva delle postazioni di lavoro;
    - defrag del disco;
    - rimozione spyware;
    - installazione di patch di sistema;
    - gestione ed aggiornamento antivirus.
- predisposizione di apparati fissi e mobili per sessioni di videoconferenza nonché supporto all'organizzazione e gestione delle sessioni, secondo le modalità indicate da Consip;
- installazione configurazione e supporto per tablet.

3.3.3 Trouble Ticketing System

Il Fornitore dovrà mettere a disposizione un Trouble Ticketing System (TTS) con interfaccia web ovvero attraverso client installato sulle PdL, in grado di accettare e gestire le richieste di assistenza provenienti dagli utenti Consip.

Il servizio di TTS deve:

- acquisire comunicazione di ogni richiesta di assistenza;
- gestione priorità ticket con colori identificativi;
- controllare stato lavorazione ticket da sito web;
- aprire ticket da email, o via web;
- dovrà essere ottimizzato per Tablet e Smartphone.

3.4 Servizi di Gestione di asset Consip

In questo capitolo sono descritte le attività di gestione degli apparati e applicativi di proprietà di Consip.

3.4.1 Gestione Rete Wireless Consip

Il Fornitore dovrà prendersi carico della gestione della rete wireless in tecnologia Wi-Fi IEEE 802.11 a/b/g/n nella banda di frequenza non licenziata 2,4 GHz presso e di proprietà Consip.

La rete ha lo scopo di garantire l'accesso in tecnologia Wi-Fi ai servizi Internet, per tutti gli utenti autenticati, e quelli messi a disposizione dalla Intranet per i soli dipendenti attraverso apparati dotati di connettività IEEE 802.11 b/g/n in banda 2,4 GHz, quali computer portatili, smartphone, tablet.

La rete Wi-Fi è composta dai seguenti elementi :

- Nr. 50 Access Point (AP), dispositivi che permettono al client di collegarsi ad una rete wireless;
- Un Wireless Controller, cioè apparato che svolge la funzione di nodo centralizzato di switching e di gestione per tutta la rete Wi-Fi a cui sono collegati tutti gli AP.

Tali apparati dovranno essere gestiti rispettando gli SLA riportati in Appendice 1.

3.4.2 Gestione dell'Active Directory

Il servizio di Gestione delle utenze è erogato tramite infrastruttura di proprietà di Consip.

Al Fornitore è richiesta la gestione di questa componente infrastrutturale nonché la definizione e manutenzione delle policy che documentano le modalità di gestione delle utenze.

Il Fornitore inoltre dovrà prevedere nel CS un Active Directory che sia la copia dell'infrastruttura di proprietà Consip.

Le attività richieste nell'ambito di questo servizio prevedono:

- supporto nella definizione e gestione delle policy legate a domini;
- supporto nella definizione delle "naming convention" da usare per tutte le risorse in rete;
- gestione (aggiungere/modificare/eliminare) delle utenze;
- gestione policy;
- gestione dei diritti di accesso alle risorse in rete di specifici utenti o gruppi di utenti;
- gestione delle "naming convention" da usare per tutte le risorse in rete;
- monitoraggio degli eventi (es. tentativi falliti di accesso ad una risorsa);
- gestione degli interventi di correzione/ripristino.

3.4.3 Gestione UTM

Il Fornitore dovrà prendere in gestione il sistema UTM installato presso Consip. Il sistema in uso è una suite di prodotti FortiNet, che svolge numerose attività di sicurezza sulla rete Consip (es. Firewall, VPN, Traffic Shaping, Intrusion Prevention System, Antivirus, Antispyware, Antimalware, Web filtering, WAN Optimization).

Il Fornitore dovrà occuparsi del suddetto apparato con personale qualificato e certificato in grado di effettuare almeno le seguenti attività di configurazione riportate a titolo esemplificativo e non esaustivo:

- nuove politiche di sicurezza;
- attivazione utenti;
- controllo rete Wi-Fi;
- gestione delle componenti antivirus centrali e locali;
- gestione dei log.

Il Fornitore dovrà attivarsi, in caso di guasti, o di malfunzionamenti che necessitano una assistenza specialistica del produttore, chiamando o aprendo un ticket presso il servizio assistenza specifico FortiNet fornendo eventuali log di sistema o supporto sistemico concordato con il produttore atto a risolvere nel più breve tempo possibile il malfunzionamento. Si rende noto che i costi per la sottoscrizione annuale al servizio di assistenza e manutenzione h24 dei prodotti FortiNet saranno a cura della Consip stessa.

3.4.4 Gestione Sistema Backup & Restore delle PdL

Per quanto riguarda il sistema di Backup delle PdL il Fornitore dovrà gestire gli apparati e gli applicativi presenti nella sede di Consip.

Il dispositivo messo a disposizione da Consip è un prodotto EMC che svolge i compiti di backup delle PdL. Questo prodotto è un sistema hardware corredato da uno specifico agent di backup che offre backup completi.

Il Fornitore dovrà prendere in gestione tale sistema occupandosi sia della modifica delle policy di backup sia creazione di gruppi o utenti sia della apertura di ticket verso il servizio di assistenza dell'apparato, fornendo il necessario supporto sistemico al fine di risolvere nel più breve tempo possibile il malfunzionamento. Si rende noto che i costi per la sottoscrizione annuale al servizio di assistenza e manutenzione h24 del sistema EMC saranno a cura della Consip stessa.

3.5 Servizi di Consulenza

Nel corso della fornitura saranno necessarie delle attività di consulenza specializzata come è descritto nei capitoli successivi.

3.5.1 Consulenza per la migrazione dei sistemi

Il Fornitore deve prevedere di allocare una risorsa, che funga da riferimento, per tutta la durata delle attività di migrazione dall'attuale infrastruttura Consip verso quella del Fornitore. Tale figura professionale verrà identificata come *"Consulente per la migrazione tecnologica"* e sarà descritta dettagliatamente in Appendice 2.

A seguito della stipula del contratto, il Fornitore, coordinandosi con i responsabili Consip, dovrà presentare un Piano di Migrazione dettagliato dove verranno definite in modo puntuale le modalità di attivazione dei singoli servizi attualmente utilizzati e tutte le informazioni richiamate nei paragrafi precedenti. A seguito del collaudo funzionale della intera infrastruttura, il Fornitore dovrà fornire il supporto specialistico e realizzare le attività necessarie alla definizione dell'architettura di rete per la fornitura.

In fase di chiusura della fornitura ovvero nei casi di migrazioni totali o parziali verso fornitori alternativi il Fornitore dovrà garantire, attraverso sufficienti figure professionali, un'attività di consulenza che consenta di spostare l'infrastruttura Consip, ospitata nel CS del Fornitore verso quella del nuovo Aggiudicatario della fornitura. La definizione ed i requisiti di tali figure professionali sono dettagliate in Appendice 2.

Figura Professionale	**Percentuale di utilizzo (mix)**
System integrator	65,00%
Specialista di Prodotto/Tecnologia	25,00%
Sistemista senior	10,00%

3.5.2 Consulenza specialistica

Nel corso della fornitura la Consip potrà richiedere servizi di consulenza specialistica a consumo. Attraverso tale servizio la Consip avrà a disposizione risorse specializzate che possano risolvere problematiche specifiche per l'acquisto, modifiche, personalizzazioni dei servizi.

Si stima che il numero massimo di giornate che potranno essere richieste è pari a 150, sulla base di un mix di figure professionali. La definizione ed i requisiti di tali figure professionali sono dettagliate in Appendice 2.

Figura Professionale	**Percentuale di utilizzo (mix)**
Capo Progetto	20,00%
Analista Funzionale	40,00%

Specialista di Tematica	15,00%
Specialista di Tecnologia/Prodotto	25,00%

3.6 Attività Sistemistica

Per svolgere tutte le attività di modifica dei sistemi il Fornitore dovrà mettere a disposizione delle figure professionali, quali Sistemista Junior e Sistemista Senior e Sistemista di rete, con le caratteristiche descritte nell'appendice 2.

4. REQUISITI DELLA FORNITURA

L'erogazione dei servizi indicati nel presente Capitolato Tecnico richiede che il Fornitore operi attraverso un Centro Servizi, che dovrà soddisfare tutti i requisiti specificati nei successivi paragrafi. La progettazione, realizzazione e gestione dei servizi dovrà obbligatoriamente essere tale da soddisfare criteri di alta affidabilità, disponibilità e resistenza mediante soluzioni ridondate (ad esempio mirroring, clustering, load balancing) su tutte componenti essenziali dell'infrastruttura.

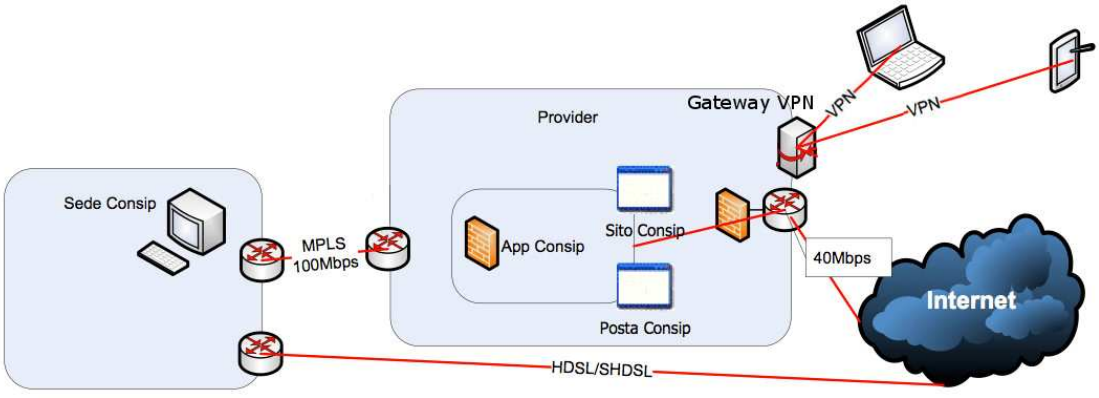
L'infrastruttura dovrà obbligatoriamente essere attiva H24 per 365 giorni l'anno. La gestione e la manutenzione ordinaria della stessa (ad esempio installazioni di patch di sicurezza, service pack, riorganizzazione di DB) non dovrà di norma produrre disservizi all'utente. Eventuali fermi programmati per la manutenzione straordinaria dovranno essere concordati e autorizzati da Consip.

Il Fornitore dovrà garantire, per l'intera durata contrattuale, l'evoluzione tecnologica dell'infrastruttura HW e della piattaforma SW (ad esempio manutenzioni correttive, evolutive, avanzamenti di versioni, ecc.) senza oneri aggiuntivi per Consip. Gli strumenti hardware, i sistemi operativi, le infrastrutture di virtualizzazione comprensive delle eventuali licenze necessarie all'erogazione e alla fruibilità dei servizi saranno a carico del Fornitore.

I prodotti SW proposti dal Fornitore dovranno essere all'ultimo livello di versione disponibile al momento della presentazione dell'offerta.

4.1 Requisiti di Connettività

Si richiede al Fornitore di implementare una Rete ad alte prestazioni di pacchetti IP attraverso una rete condivisa basata sullo standard Multi Protocol Label Switching (MPLS) tra il proprio CS e la sede Consip secondo tutto quanto previsto dal precedente paragrafo 3.1.



Il Fornitore dovrà fornire almeno 10 Indirizzi Pubblici.

4.2 Requisiti del Centro Servizi per l'Erogazione del Servizio di Hosting

Il Fornitore dovrà mettere a disposizione dei Data Center, impegnati per la fornitura, con connessioni multiple dirette in fibra ottica ai principali carrier italiani ed esteri oltre al collegamento ai due NAP (Neutral Access Point) nazionali MIX di Milano ed al NaMeX di Roma. L'architettura di backbone geografico e metropolitano del Fornitore, che interconnette le varie sedi dei Data Center dovrà consentire di delocalizzare i servizi con la massima affidabilità e sicurezza. La dislocazione in aree territoriali diverse dei Data Center è requisito fondamentale per offrire servizi di disaster recovery.

Il CS proposto per la fornitura dovrà essere ospitato all'interno della struttura dei Data Center messi a disposizione del Fornitore.

Il CS del Fornitore dovrà impiegare soluzioni di fault-tolerance per tutte le connessioni garantendo la continuità del servizio in caso di incidenti sia delle dorsali nazionali che internazionali, assicurando una banda di accesso sempre disponibile, fornita nel rispetto degli standard qualitativi più stringenti e in grado di assicurare altissime prestazioni e affidabilità.

Il CS dovranno essere caratterizzati da misure di identificazione e controllo degli accessi, presidio continuo, monitoraggio 24h/24h per 365 giorni da parte del Network Operating Center (NOC) del Fornitore. L'accesso alle strutture sarà autorizzato unicamente in presenza del personale tecnico del Fornitore e sistemi di telecamere a circuito chiuso e sensori di presenza impediranno gli accessi fisici non autorizzati.

Il CS dovrà offrire server fisici, eventualmente richiesti da Consip, e dovrà essere strutturato per poter realizzare soluzioni standard di virtual server, caratterizzate da elevata affidabilità e sicurezza (ad oggi è utilizzata la piattaforma VMware).

Il data center dovrà garantire inoltre i servizi di:

- monitoraggio 24h/24h x 365 giorni l'anno su reti, sistemi e applicazioni;
- installazione, manutenzione e assistenza personalizzati;
- possibilità di accedere a servizi di carrier alternativi;
- procedure di accesso e registrazione nominali per tutte le operazioni svolte all'interno.

4.2.1 Requisiti dei Servizi di Hosting

Il Fornitore dovrà predisporre all'interno del CS un opportuno numero di server fisici e virtuali tali da poter ospitare tutti sistemi menzionati nei paragrafi precedenti gli applicativi sviluppati in Consip. Per semplicità riportiamo una tabella riassuntiva dei fabbisogni per ospitare le applicazioni descritte nel paragrafo 3.2.1 e seguenti. Se non diversamente indicato le macchine elencate di seguito si intendono virtuali.

	Esercizio		Collaudo/Test	
Application Servers	**Midrange**	**Entry level**	**Midrange**	**Entry level**
Jboss + Tomcat	2		1	
IIS6	2		1	
Coldfusion		2		1

Database	**Midrange**	**Entry level**	**Midrange**	**Entry level**
SQL Server (2012)	2		1	
SQL Server (2005)	2		1	
MySQL		1		1

Sistemi	**Midrange1**	**Entry level**	**Midrange**	**Entry level**
Gestione Documentale	3	1		3
DISCO		1		
Altri Sistemi	5	5		

Componenti Infrastrutturali	**Midrange**	**Entry level**	**Midrange**	**Entry level**
Active Directory		2		
Power Center	1		1	
File Server		2		1

Per quanto riguarda i server si richiede che tali server abbiano le seguenti caratteristiche minime:

Server Entry Level

- CPU a 64 Bit in tecnologia x86 ovvero con caratteristiche assimilabili a una CPU Intel Xeon serie 5600;
- 2 - 4 CPU, in caso di server virtuali, garantite almeno al 50%;
- 4 – 8 GByte RAM
- almeno 2 porte compatibili con Network Gigabit-Ethernet 10/100/1000 Mbps;
- spazio disco interno RAID5 almeno 500GB ed eventualmente spazio disco allocabile dinamicamente dalla SAN;
- Sistema Operativo[1].

[1] Windows, RedHat, CentOS.

Server Midrange

- Virtual CPU a 64 Bit in tecnologia x86 ovvero con caratteristiche assimilabili a una CPU Intel Xeon serie 5600;
- 4 - 8 CPU , in caso di server virtuali, garantite almeno al 50%;
- 16 – 32 GByte RAM
- almeno 3 porte compatibili con Network Gigabit-Ethernet 10/100/1000 Mbps;
- spazio disco interno RAID5 almeno 500GB ed eventualmente spazio disco allocabile dinamicamente dalla SAN;
- Sistema Operativo[2].

Su richiesta di Consip i Server dovranno essere organizzati in cluster utilizzando sia gli strumenti software previsti dai sistemi operativi sia apparati di rete esterni che opereranno il bilanciamento di carico.

Il numero di server censito nella tabella precedente risulta essere di:

- 22 server Midrange;
- 20 server Entry Level.

Si stima che, al momento della stipula, verrà richiesta l'attivazione di un numero massimo di server così come sopra riportato, fermo restando che, nel corso della durata contrattuale, la Consip potrebbe richiedere un aumento della dimensione del detto servizio fino ad un massimo di 33 server Midrange e 30 server Entry Level.

Il Fornitore dovrà prevedere di svolgere all'interno del CS tutte le attività di gestione sistemistica dei server e degli ambienti ospitati. Si riporta di seguito la descrizione delle principali attività che dovranno essere garantire per l'erogazione dei servizi:

- predisposizione dell'infrastruttura in termini di installazione e messa in funzione di nuovi sistemi quali, ad esempio, server, client, software di base e relativo software d'ambiente (middleware) nonché di nuovi apparati per l'erogazione di servizi di rete, integrandoli ove necessario con i servizi di telecomunicazioni (TLC);
- upgrade di sistemi gestiti, in termini di creazione di nuovi ambienti e di modifiche della configurazione dei sistemi sia in termini hardware che software non riconducibili ad attività di ordinaria gestione e manutenzione, e della loro ottimizzazione nonché le modifiche alle interconnessioni ed al modello architetturale ed il correlato modello operativo/gestionale dei sistemi;
- in caso di upgrade, gli aggiornamenti di sistema dovranno avere una schedulazione mensile e dovranno essere preventivamente installati sulle macchine nell'Ambiente di Sviluppo, Collaudo e Certificazione delle Patch per una valutazione d'impatto. Infine, su input di Consip gli aggiornamenti dovranno essere passati sui sistemi di produzione.

[2] Windows, RedHat, CentOS.

In caso di particolari situazioni di necessità dovrà essere possibile attivare un task di aggiornamento specifico.

- ottimizzazione delle reti nonché le modifiche delle connessioni tra i nodi di rete e conseguente aggiornamento delle configurazioni delle applicazioni/sistemi ove la modifica abbia un impatto su di esse;
- la produzione di tutta la documentazione relativa alle nuove infrastrutture e alle evoluzioni delle infrastrutture pre-esistenti nonché la fornitura di tutte le informazioni necessarie per il corretto uso dei prodotti/sistemi installati.

La predisposizione dell'infrastruttura comprende l'installazione e la configurazione degli agent necessari per il monitoraggio e/o il tuning e/o il capacity planning dei sistemi. Inoltre, potrà essere richiesto al Fornitore fornisca supporto sistemistico ai progetti applicativi, al fine di definire tutte le componenti infrastrutturali e architetturali di progetto.

4.2.2 Requisiti dei servizi esternalizzati

4.2.2.1 *Requisiti Protocollo Informatico*

Il Fornitore dovrà erogare un servizio di protocollazione informatica che consenta la registrazione di protocollo per ogni documento ricevuto o spedito in conformità con l'articolo 53 del D.P.R. 445/2000 che dovrà rispettare quanto indicato nel paragrafo 3.2.2.1 avere almeno le seguenti caratteristiche minime:

- numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico (Firma Elettronica), se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

Il Fornitore dovrà erogare tale servizio che avrà, presumibilmente, un dimensionamento pari a circa 25000 documenti annui per una dimensione massima di 100 GigaByte;

4.2.2.2 *Requisiti della Conservazione Sostitutiva*

Si richiede al Fornitore di erogare tale servizio di conservazione sostitutiva secondo quanto già indicato al paragrafo 3.2.2.2 ed in accordo con le "*Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali*" (Deliberazione CNIPA n. 11/2004 del 19 febbraio 2004).

Il Fornitore dovrà erogare tale servizio che avrà, presumibilmente, un dimensionamento pari a circa 25000 documenti annui per una dimensione massima di 100 Gigabyte.

4.2.2.3 *Requisiti del File Server*

Si richiede al Fornitore di predisporre nel Centro Servizi un File Server le cui dimensioni minime dovranno essere di 3 TByte[3]. Solo a titolo di esempio riportiamo alcune funzionalità che dovrà avere il file server:

- attivazione/disattivazione di cartelle di lavoro;
- abilitazione/disabilitazione di utenti di dominio alle singole cartelle;
- spazio di archiviazione facilmente scalabile;
- gestione Distributed File System (DFS);

Inoltre il fornitore dovrà garantire le seguenti attività:

- esecuzione periodica dei backup del file server;
- restore di file da una cartella condivisa su richiesta di Consip;
- manutenzione periodica del file server;
- monitoraggio delle performance del file server, dello spazio disponibile sul file server, prevenzione della saturazione dei file system.

4.2.3Requisiti dei Servizi hosting esposti verso l'esterno

Per quanto riguarda l'accesso al sito web da parte degli utenti finali si ipotizzata una contemporaneità degli accessi pari approssimativamente a 100 utenti finali. Per garantire la gestione di eventuali picchi di traffico non preventivabili e superiori alla stima il Fornitore dovrà consentire un collegamento Internet di banda fino a 12 Mbps per la fruizione da Internet dei contenuti del sito.

Si stima che, al momento della stipula, verrà richiesto uno spazio fisico occupato dal sito web pari a 40GB.

Il Fornitore dovrà monitorare costantemente l'occupazione della banda e provvedere ad incrementarne la disponibilità con l'aggiunta di ulteriori flussi IP secondo politiche di capacity planning che garantiscano i più elevati livelli di servizio.

Il servizio di hosting del sito web deve prevedere le seguenti caratteristiche gestionali:

Servizi di sicurezza di rete (Firewall e Intrusion Prevention) tali servizi devono contribuire a proteggere il sito web ospitato da attacchi di rete e devono tenere traccia, tramite specifici Log, di tutte le attività anomale individuate;

[3] La capacità dello spazio potrà essere direttamente presa dallo spazio SAN.

Servizio Web Application Firewall (WAF) deve contribuire a proteggere il sito web ospitato da attacchi di livello applicativo e deve tenere traccia, tramite specifici Log, di tutte le attività anomale individuate;

Servizio di Gestione Incidenti in base al quale eventuali attività malevole tentate o portate a termini nei confronti del sito dovranno essere notificate a Consip. Le successive attività de gestione del incidente dovranno essere gestite secondo quanto descritto nel paragrafo 3.2.5.2;

Servizio di gestione dei Log, su richiesta di Consip dovranno essere prodotti i log delle componenti del sistema su cui è realizzato il sito web (web server, DB, e componenti di sicurezza). Tali log dovranno essere forniti secondo modalità e su supporti che consentano di produrli come allegati di denunce alle autorità competenti.

4.2.4Requisiti di Sicurezza Logica

Il Fornitore dovrà predisporre la sua organizzazione tutte le tecniche e le modalità operative per mettere in sicurezza i dati di Consip come definito nelle norme ISO 27000 dedicate agli standard per la sicurezza informatica. Il Fornitore dovrà implementare al suo interno un sistema di gestione di sicurezza tale da prevenire o ridurre attacchi informatici.

A tale scopo dovrà configurare apparati di Firewall, NIDS, NIPS, Antivirus, VPN.

4.2.4.1 *Firewall*

Il Fornitore deve garantire almeno le seguenti caratteristiche di base per il servizio di firewalling:

- Filtraggio di traffico IP: consente di proteggere una rete IP o singole postazioni di lavoro da accessi indesiderati bloccando indirizzi, porte e protocolli.
- Auditing e logging: consente l'analisi del traffico che attraversa il firewall.
- Modulo di ispezione: effettua l'ispezione dei datagrammi IP e realizza il filtraggio sulla base delle regole implementate. Dovrà essere implementata la metodologia "stateful inspection".
- Modulo di gestione: è il componente funzionale che consente di configurare e monitorare il comportamento del sistema firewall.
- Gestione dell'accessibilità di specifici servizi sulla base della profilazione utente (user, mobile user, vpn user)
- Gestione dell'autenticazione e controllo degli accessi: consente di regolare l'impiego di alcuni servizi (FTP, Telnet, http, Https) veicolati per il tramite del firewall sulla base di una preventiva autenticazione.
- Network Address Translation (NAT) secondo la specifica RFC-3022, sia di tipo statico (uno a uno) sia di tipo dinamico (N a uno).
- Port Address Translation (PAT) Management: consente di nascondere, al fine di aumentare il livello di protezione, le porte effettive di ascolto di un sistema server protetto dal firewall, con porte fittizie.

Il sistema di firewalling dovrà implementare meccanismi di rilevazione e protezione per i più comuni attacchi di tipo Denial of Service.

Il sistema di firewalling dovrà rilevare e registrare i tentativi di accesso non autorizzati al sistema stesso.

I dati registrati dal sistema di firewalling dovranno essere disponibili per l'uso da parte degli utenti abilitati.

4.2.4.2 *Requisiti NIDS & NIPS*

Il Fornitore deve erogare un servizio di implementazione e gestione di sistemi di rilevamento delle intrusioni (Network Intrusion Detection System, NIDS) che consenta di identificare positivamente tutte le sequenze di eventi, condotti da una o più entità non autorizzate, aventi come obiettivo la compromissione di un sistema, di un apparato o della rete Consip.

Il Fornitore dovrà prevedere che la sua soluzione di NIDS abbia almeno i seguenti componenti:

- Sensore: raccoglie dati dalla rete (pacchetti dati) e li inoltra all'Analyzer. I sensori devono poter monitorare segmenti di rete con prestazioni pari a 10 Mb/s (Ethernet), 100 Mb/s (Fast-Ethernet) e 1000 Mb/s (Gigabit Ethernet);
- Analyzer: sistema centralizzato di raccolta ed analisi dei dati, in grado di rilevare un'avvenuta intrusione. Tale dispositivo riceve input da uno o più sensori o da altri analyzer, e determina l'occorrenza di una situazione di attacco. L'output di questo componente rappresenta un'indicazione di avvenuta intrusione da cui possono scaturire azioni automatiche configurabili;
- Interfaccia di gestione: interfaccia che consente di monitorare il comportamento del sistema di Intrusion Detection;
- Backdoor detection: analisi delle interazioni tra sistemi interni ed esterni per la rilevazione di "backdoor" che consentono di bypassare le procedure di sicurezza attivate nel sistema.

Il Fornitore deve garantire almeno le seguenti funzionalità del NIDS:

- supporto dei protocolli IEEE Ethernet, Fast-Ethernet, Gigabit Ethernet e tutti i protocolli specificati nello standard TCP/IP;
- analisi passiva di un protocollo tramite l'uso di sniffer;
- capacità di rilevazione degli attacchi garantendo la percentuale di falsi positivi e falsi negativi definita da specifici Livelli di Servizio;
- raccolta e conservazione delle tracce accurate degli avvenuti attacchi allo scopo di favorire l'individuazione degli autori dell'attacco e come deterrente per scoraggiare ulteriori azioni ostili;
- raccolta di informazioni sugli eventi di attacco da una o più sorgenti di informazione tramite "sensori" posti sulla rete;
- analisi predeterminata degli eventi rilevati attraverso l'utilizzo di "signature analysis" che consentono di riconoscere le serie di pacchetti al fine di riconoscere un tipico pattern rappresentativo di un attacco;

- gestione del database delle "signature";
- notifica specifica a fronte dell'identificazione di un evento di attacco;

Il Fornitore dovrà implementare e gestire anche un sistema di Intrusion Prevention, che sostanzialmente rappresenta un'estensione del servizio di NIDS, in quanto prevede la realizzazione e gestione di un sistema di prevenzione delle intrusioni che consente di identificare ed interrompere azioni aventi come obiettivo la violazione o compromissione del funzionamento di un sistema, di un apparato o di una rete.

4.2.5Requisiti sicurezza fisica

Il Fornitore dovrà garantire la conformità del CS ai principali standard di sicurezza internazionali ed implementano un Sistema di Gestione della Sicurezza delle Informazioni certificato ISO27001.

Di seguito riportiamo le condizioni minime di sicurezza dei Data Center del fornitore per ospitare il CS Consip.

Per quanto concerne la sicurezza fisica, il CS deve essere in grado di:

- Discriminare gli accessi garantendo l'ingresso alle aree riservate alle sole persone autorizzate;
- Preservare l'integrità e la disponibilità del servizio mediante soluzioni di continuità elettrica, della rete LAN, sistemi antincendio, antiallagamento e di dissipazione termica.

In particolare il sistema di controllo accessi dovrà prevedere:

- Sistema di anti-intrusione perimetrale che preveda telecamere di sorveglianza, sensori di movimento, uscite di sicurezza allarmate;
- Sorveglianza 24 ore al giorno, per tutti i giorni dell'anno;
- Sistema di Controllo Accessi esterno (tornelli, vetri blindati, porte allarmate);
- Sistema di Controllo Accessi interno su aree CED o IDC ad alto rischio.

Per quanto riguarda la tutela delle apparecchiature dovrà prevedere:

- Cablaggi delle linee di trasmissione e degli armadi di distribuzione che inibiscano inserimenti, rimozioni o manomissioni accidentali e/o non autorizzati ;
- Garanzia della continuità elettrica con sistemi a doppia cabina di distribuzione, gruppi di continuità UPS/Gruppi Elettrogeni ad azionamento automatico. ;
- Sistemi di rivelazione fumo e sistemi anti incendio in conformità con le leggi e normative vigenti (D.Lgs. 626/1994 e D.M. 10 marzo 1998) e secondo le prescrizioni dei VVFF;
- Porte tagliafuoco allarmate;
- Sistemi anti-allagamento al di sotto del pavimento flottante;
- Sistemi di condizionamento con fail-over e load-balancing in modo che i valori di temperatura e umidità siano ottimali per l'esercizio degli apparati siano controllati e mantenuti da sistemi di condizionamento e ventilazione;

- Sistemi di allarme perimetrale;

Per quanto riguarda le caratteristiche tecniche strutturali dovrà prevedere:

- Spazio disponibile all'interno di rack con doppie linee di alimentazione;
- Potenza elettrica erogabile per singolo rack fino a 7Kw;
- Pavimento flottante: 100% del totale;
- Cabine MT di trasformazione indipendenti a doppia trasformazione (N+1, active - standby)
- Gruppi di continuità (UPS) in parallelo in configurazione N+1
- Generatori indipendenti in generazione continua in configurazione N+1 (mutuo intervento), con cisterna addizionale interrata;

4.2.6 Requisiti di Configuration e Change Management

Il Fornitore dovrà prevedere al suo interno l'istituzione di un Control Center che si occupi di monitorare e gestire le infrastrutture ICT e i servizi ospitati nel CS. Il Control Center dovrà operare sui Sistemi Operativi, effettuando la gestione ordinaria e straordinaria dei server e dei servizi Consip rendendosi parte attiva fondamentale nel processo di Change Management. Il personale tecnico (Sistemista Senior, Sistemista Senior di Rete, Sistemista Junior) impiegato nel Control Center dovrà rispondere ai requisiti minimi definiti in Appendice 2.

Nell'ambito del processo di Change Management sono tipicamente identificate tre tipologie di change:

- Change Standard: per i quali esiste già una definizione ben strutturata e documentata della modifica da effettuare. Tali tipi di change sono definibili a priori con template che contengono il flusso definito per l'implementazione che, riguardando attività predefinite, ripetibili ed a basso impatto e rischio, necessitano di un iter approvativo ridotto, relativo ad esempio agli aspetti di pianificazione della data in cui effettuare le attività necessarie.
- Change non Standard: per i quali sono richieste modifiche non comuni e predefinite ma piuttosto complesse, per le quali è necessaria un'analisi preliminare di impatto volta a definire le attività da svolgere con un piano di lavoro specifico.
- Emergency: change che nascono dalla necessità immediata di risolvere un incidente, siano essi standard o complessi, ma che per la particolare natura di urgenza/emergenza (ad esempio risolvere una situazione di crisi) hanno la necessità di essere implementati senza una fase di approvazione formale per non bloccare le attività.

Il Control Center dovrà occuparsi del patching dei SO e degli applicativi con cadenza mensile, salvo situazioni di particolare esposizione alla sicurezza e richieste specifiche di Consip.

Il Fornitore dovrà definire, all'intero del Piano di Migrazione, un piano degli interventi che verrà concordato con la Consip, dove verranno evidenziate tutte le tempistiche delle varie tipologie di interventi (change standard, change non standard, emergency), in modo che sia possibile verificare che le funzionalità dei servizi dati in hosting siano garantite.

Le attività di patching di natura complessa dovranno essere comunque precedute da una analisi di impatto ed una fase di approvazione, prima del rilascio sui sistemi, che coinvolgerà anche Consip. Tali attività verranno eseguite in orario lavorativo standard (lun-ven; 08:00-18:00), a meno di situazioni di particolare gravità che verranno gestite su esigenza specifica.

4.3 Assistenza

Il Fornitore dovrà definire al suo interno un **Responsabile del servizio di Assistenza** che sarà il punto di contatto per tutte le attività necessarie alla erogazione dei servizi di assistenza per gli ambienti server, le PdL, agli apparati Consip dati in gestione.

4.3.1Requisiti del Service Desk

Il Fornitore dovrà offrire una gestione centralizzata di tutte le richieste pervenute da Consip relative alla gestione ordinaria o straordinaria dei servizi dati in hosting, nonché di malfunzionamenti e anomalie per garantire la fruibilità dei servizi. Il Service Desk dovrà essere a disposizione di Consip nelle fasce orarie Lunedì - Venerdì, 8:00-22:00 e sabato 8:00-14:00 e dovrà prevedere la sua raggiungibilità sia attraverso un numero verde che via TTS.

Il Service Desk dovrà:

- ricevere le richieste pervenute da Consip;
- attivarsi per l'intervento necessario coordinando le opportune strutture di supporto tecnico al suo interno;
- controllare lo stato di avanzamento dei ticket immessi;
- garantire il rispetto degli SLA previsti nel piano di interventi concordato per quanto riguarda i change standard, change non standard, Emergency;
- garantire aggiornamenti periodici sulle richieste in corso ad un referente di Consip;
- informare Consip del completamento della richiesta.

Nel caso di guasti bloccanti o altre richieste urgenti, il Fornitore dovrà prevedere una procedura di escalation articolata su vari livelli che consente al referente di Consip di contattare il Service Manager o, in ultima analisi, i responsabili del Fornitore delle strutture preposte alla gestione del servizio.

4.3.2Requisiti Help Desk

Il Servizio di Help Desk dovrà essere strutturato in modo da poter intervenire in tempi brevi attraverso personale tecnico in grado di risolvere direttamente il problema.

L'Help Desk dovrà essere contattato attraverso: accesso telefonico, via web (TTS), email.

Il servizio dovrà garantire la presenza presso la sede di Consip di personale tecnico (2 FTE) da Lunedì - Venerdì, nelle fasce orarie 8:00-18:00.

Il numero di risorse allocate dovrà essere sufficiente a sostenere il traffico di chiamate entranti ed il rispetto degli SLA previsti nel piano di interventi concordato per quanto riguarda i change standard, change non standard, Emergency.

Il servizio di Help Desk di primo livello si occuperà di ricevere le segnalazioni di malfunzionamento attraverso i canali già citati, individuarne la complessità attribuirne la classe (standard o non standard) e quindi assegnargli una priorità di intervento.

4.3.2.1 *Requisiti Presidio tecnico PdL*

La Gestione del parco delle Postazioni di Lavoro (PdL) avviene attraverso il predetto personale dislocato presso la sede di Consip di personale tecnico (2 FTE) che si occuperanno di gestire:

- le attività di gestione fisica del parco PdL;
- gli interventi a supporto degli utenti, anche in remoto, per la gestione delle varie tipologie di malfunzionamenti che si possono presentare;
- un confronto tecnico costante con gli altri Presidi interni, che hanno in carico la gestione dei server, delle reti, e dei servizi di sicurezza;
- un rapporto diretto con i responsabili Consip, per la pianificazione e le sincronizzazione delle attività per la gestione delle PdL (es. upgrade, sostituzioni, software distribution).

4.3.3Requisiti del TTS

Il Trouble Ticketing System deve consentire all'utente di inserire le proprie richieste (segnalazioni anomalie, richieste di servizio, richieste di cambiamenti, etc.) tramite una interfaccia web e tramite la stessa controllare lo stato delle proprie richieste e apportare aggiornamenti.

Il servizio TTS dovrà fungere da punto di contatto sia per le richieste di assistenza alle PdL, sia per l'assistenza dei servizi offerti dal Centro Servizi che verranno inviate al personale tecnico del Control Center.

L'utilizzo di tale strumento assicura l'efficacia e l'efficienza delle attività di assistenza per Consip. A titolo di esempio riportiamo alcune funzionalità:

- possibilità di accesso all'applicazione da tutte le PdL con le proprie credenziali di accesso integrate nel dominio Active Directory;
- apertura e gestire ticket di incident. I ticket di incident fanno riferimento a malfunzionamenti o comunque a funzionamenti che si discostano dalla normale operatività;
- apertura e gestione ticket di change request. Le change request sono richieste di modifiche al servizio erogato oppure richieste che, per essere soddisfatte, prevedono la modifica delle configurazioni in essere (es. update della configurazione sw,…);
- apertura ticket per gestione/manutenzione/upgradare i server virtuali e fisici e i loro sistemi operativi;
- apertura ticket per la gestione i middleware ed i software di base;
- ricezione richieste di servizio, ovvero richieste, da parte di Consip, di una prestazione contrattualizzata;

- effettuazione sugli interrogazioni sugli incident, i problem e le change e produzione la relativa reportistica;
- controllo lo stato di avanzamento dei ticket immessi;
- monitoraggio i tempi di lavorazione dei ticket e relativa correlazione a soglie definite nel piano degli interventi in funzione dei livelli di servizio contrattualizzati.

4.4 Reportistica

Il Fornitore dovrà produrre dei report dettagliati delle attività svolte nel periodo di riferimento, dove si potranno evincere anche le tempistiche di intervento o gli up-time dei servizi.

4.4.1 Console di monitoraggio

Il Fornitore dovrà mettere a disposizione una console per monitorare la disponibilità e le prestazioni dei servizi offerti tramite il Centro Servizi in modo che sia possibile una migliore gestione dell'IT e dei processi IT. La Console dovrà quindi fornire il monitoraggio di varie applicazioni, database, siti web, applicazioni Web, server di posta e altri servizi IT aziendali in accordo con gli SLA descritti nelle appendici.

4.5 Requisiti delle Attività Sistemistiche

Il Fornitore dovrà fornire delle figure professionali adatte a svolgere le attività sistemistiche Change Standard, Change non Standard, Emergency come definite in Appendice 2.

I tempi per i Change Standard, non standard ed Emergency saranno concordati con Consip all'interno del piano degli interventi così come descritto al paragrafo 4.2.6.

5. GESTIONE DELLA FORNITURA

Alla stipula del Contratto, il Committente (Consip) illustrerà le attività da svolgere, indicando le informazioni e le scadenze note, i piani di evoluzione dei sistemi e ogni altra informazione utile ad una corretta pianificazione.

A partire dalla data di stipula, il Fornitore potrà richiedere il supporto di Consip o di terzi da esso designati (es. Fornitore uscente, Fornitore per la gestione applicativa, Fornitore di servizi oggetto di supporto, etc.), al fine di acquisire le conoscenze necessarie per la presa in carico dei servizi relativi a ciascun ambito e per un loro corretto svolgimento, per un periodo massimo pari a **45 (quarantacinque) giorni solari**.

Durante tale medesimo periodo il Fornitore è tenuto a produrre il **Piano di Migrazione** che deve essere sottoposto all'approvazione di Consip.

Il Fornitore è tenuto in tale periodo ad acquisire il know how necessario finalizzato alla presa in carico e all'espletamento dei servizi e delle attività previste nel presente capitolato.

Per tutto il periodo di affiancamento di inizio fornitura, il Fornitore non percepirà alcun corrispettivo.

Il Fornitore dovrà nominare le seguenti figure professionali funzionali alla gestione della fornitura:

- un "Referente Generale della Fornitura";
- un "Responsabile del Centro Servizi";
- un "Responsabile della sicurezza dei servizi erogati dal Centro Servizi";
- un "Responsabile del servizio di Conservazione Sostitutiva";
- un "Responsabile del Servizio di Assistenza".

Tali figure professionali, descritte con maggiore dettaglio nei paragrafi successivi, sono funzionali ad una corretta erogazione dei servizi richiesti nel presente Capitolato, per tale motivo si considerano parte integrante della Fornitura e non comporteranno alcun onere aggiuntivo per Consip.

5.1 Referente Generale della Fornitura

Il **Referente Generale della Fornitura** non farà parte di alcuno dei gruppi di lavoro individuati per i vari servizi descritti nel presente Capitolato.

Il Referente Generale della Fornitura avrà la responsabilità delle seguenti attività:

- curare i rapporti con Consip;
- fornire le informazioni richieste da Consip, relativamente alla presa in carico e gestione delle problematiche emerse nell'ambito dell'esercizio del Contratto di Fornitura;
- impostare, organizzare, pianificare e controllare tutte le azioni necessarie per garantire il rispetto delle prestazioni;

- coordinare i Referenti specifici di fornitura e supervisionare le loro attività;
- monitorare l'andamento dei livelli di servizio di assistenza e manutenzione per tutto il periodo di efficacia del Contratto di Fornitura;
- gestire reclami/disservizi/segnalazioni da parte della Consip.

Si sottolinea che, a prescindere dall'organizzazione che il Fornitore adotterà per l'erogazione dei servizi, è compito del Referente Generale della Fornitura assicurare un alto grado di sinergia principalmente tra le risorse impiegate in tutti i servizi al fine di garantire un costante e adeguato grado di conoscenza e di attenzione evitando discontinuità.

In caso di inadeguatezza del Referente, Consip si riserva di chiederne la sostituzione secondo quanto prescritto nel contratto.

5.2 Responsabile del Centro Servizi

Il **Responsabile del Centro Servizi** avrà il compito di coordinare tutte le attività necessarie alla erogazione dei servizi previsti nel presente Capitolato Tecnico.

Titolo di studio

- Laurea in discipline tecniche e/o gestionali

Esperienze lavorative

- Minimo 15 anni, di cui almeno 10 nel settore informatico;
- Esperienza di almeno 5 anni nella conduzione e gestione di servizi informatici e di personale a questi assegnato;

Conoscenze

Esperienza nell'analisi delle problematiche interne ad una rete aziendale complessa, capacità progettare interventi e automatismi in grado di limitare gli imprevisti e ottimizzare le funzionalità della rete informatica. Le principali attività che dovrà svolgere sono:

- coordinare il personale/collaboratori tecnico che opera nel Data Center;
- rappresentare il punto di contatto tra Consip e il Fornitore per le problematiche della fornitura;
- conoscenza della gestione di macchine virtuali, sistemi di back-up, apparati di rete, firewall ecc..

5.3 Responsabile della sicurezza dei servizi erogati dal Centro Servizi

Il **Responsabile della sicurezza dei servizi erogati dal Centro Servizi** avrà il compito di coordinare le attività inerenti agli aspetti di sicurezza relativi ai servizi erogati.

Titolo di studio

- Laurea in discipline tecniche o cultura equivalente

Esperienze lavorative

- Minimo 7 anni, di cui almeno 4 nella funzione

Conoscenze

Conoscenza ed esperienza in ambito di amministrazione e gestione di reti e sistemi, di monitoraggio, di analisi del rischio e delle capacità di recovery. Conoscenza sulle tematiche di crittografia, e delle principali minacce informatiche. Conoscenza delle tematiche che riguardano la gestione della sicurezza fisica e delle operazioni da mettere in atto per la tutela degli apparati, conoscenza dell'architettura dei computer e dei sistemi e della sicurezza di rete di telecomunicazioni. Le principali attività che dovrà svolgere sono:

- definire le politiche di sicurezza e i livelli di autorizzazione per l'utilizzo delle risorse informatiche;
- adottare tutte le protezioni hardware e software per attuare la sicurezza attiva e passiva;
- predisporre i sistemi in modo da adempiere alle regolamentazioni del nuovo codice per la privacy e delle leggi sulla sicurezza dei dati;
- assicurare l'efficienza dei sistemi di allarme ambientali e periferici;
- assicurare l'accesso fisico e/o logico solo ad utenti autorizzati;
- consentire la fruizione di tutti e soli i servizi previsti dai singoli utenti nei tempi e nelle modalità previste dal sistema;
- garantire l'integrità e la correttezza dei dati memorizzati;

5.4 Responsabile del servizio di Conservazione Sostitutiva

Il **Responsabile del servizio di Conservazione Sostitutiva** avrà il compito di garantire che il servizio di protocollazione e conservazione sostitutiva sia sempre aderente alle norme in vigore e funzionante secondo gli SLA indicati.

Titolo di studio

- Laurea in discipline giuridiche o cultura equivalente

Esperienze lavorative

- Minimo 5 anni, di cui almeno 3 nella funzione

Conoscenze

Esperienza maturata nella gestione di servizi di conservazione della documentazione digitale, conoscenza dell'attuale normativa di riferimento e delle relative linee guida tecnico operative per la conservazione sostitutiva. Le principali attività che dovrà svolgere sono:

- Assicurare la corretta funzionalità del servizio di conservazione sostitutiva;
- archiviare e rendere disponibili i documenti mandati in conservazione;
- predisporre di copie di sicurezza;
- verificare il funzionamento corretto del sistema e dei programmi di gestione;

- adottare tutte le misure che si rendono necessarie per assicurare la sicurezza fisica e logica del sistema deputato alla conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
- garantire l'assistenza e le risorse necessarie ad un pubblico ufficiale un per il compimento delle sue in tutti i casi previsti dalla normativa;
- verificare, con cadenza periodica non superiore ai cinque anni, la leggibilità effettiva dei documenti conservati, provvedendo, quando sia necessario al riversamento diretto o sostitutivo del contenuto dei supporti.

5.5 Responsabile del Servizio di Assistenza

Il **Responsabile del Servizio di Assistenza** avrà il compito di coordinare tutte le attività necessarie alla erogazione dei servizi di assistenza, per gli ambienti server, per le PdL, per gli apparati Consip dati in gestione al Fornitore.

Titolo di studio

- Laurea in discipline tecniche o cultura equivalente

Esperienze lavorative

- Minimo 5 anni, di cui almeno 3 nella funzione

Conoscenze

Competenza ed esperienza nella pianificazione di progetti complessi, capacità di organizzazione e gestione di team di lavoro, capacità di problem solving. Le principali attività che dovrà svolgere sono:

- ricoprire il ruolo di referente del Fornitore per le attività di assistenza;
- coordinare le attività di assistenza tecnica, organizzando il servizio interno e gestendo anche le attività che verranno svolte nella sede Consip;
- rispondere alle richieste di informazione, supporto ed assistenza tecnica provenienti da Consip;
- risolvere tempestivamente problematiche ed anomalie di funzionamento coordinandosi con i tecnici/sistemisti presenti nel CS;
- pianificare e coordinare i relativi interventi sia in remoto sia direttamente sul campo, organizzando le risorse tecniche.

5.6 Assicurazione Qualità

Nell'esecuzione delle attività contrattualmente previste il Fornitore dovrà:

- rispettare i principi di gestione della qualità della norma EN ISO 9001 rispetto alla quale gli è stata richiesta la certificazione;
- attenersi ed essere conforme a quanto previsto dal "Piano di Qualità della fornitura" approvato da Consip S.p.A. e a quanto previsto dal proprio Sistema di Gestione della Qualità;

- rispettare i principi per il sistema di gestione della sicurezza delle informazioni, della norma ISO IEC 27001:2013.

Il Piano di Qualità della fornitura sarà redatto dal Fornitore e costituirà il riferimento per le attività di verifica e validazione svolte dal Fornitore all'interno dei propri gruppi di lavoro.

Entro 30 (trenta) giorni solari dalla data di stipula del contratto, il Fornitore dovrà consegnare il Piano di Qualità.

Il Piano di Qualità della fornitura, dovrà descrivere le modalità realizzative e garantirne l'adeguatezza rispetto agli obiettivi durante tutta la fornitura.

Il Piano di Qualità della fornitura dovrà essere aggiornato a seguito di significativi cambiamenti di contesto in corso d'opera o, comunque, su richiesta di Consip S.p.A. ogni qualvolta lo reputi opportuno. In questo caso dovrà essere riconsegnato l'intero documento, e non per le sole parti variate, e dovrà essere possibile individuare le modifiche effettuate.

Nella stesura del Piano di Qualità della fornitura, il Fornitore dovrà dettagliare, per ciascun requisito di qualità, le fonti dati utilizzate per la raccolta dei dati elementari e gli strumenti utilizzati per l'elaborazione delle informazioni di dettaglio.

Il Piano di Qualità della fornitura sarà sottoposto all'approvazione di Consip S.p.A., che potrà notificare eventuali rilievi.

Nel caso in cui il Fornitore, certificato rispetto alla norma EN ISO 9001, non risolva i rilievi notificati da Consip S.p.A. sul Piano di Qualità della fornitura, la Consip S.p.A. si riserva di effettuare un'apposita segnalazione all'ente Certificatore.

Le successive versioni o revisioni del Piano di Qualità della fornitura saranno consegnate in funzione delle variazioni intervenute.

5.6.1Piano della Qualità della Fornitura

Per la redazione del Piano di Qualità della Fornitura si riporta, a titolo esemplificativo, uno schema che potrà essere utilizzato dal Fornitore come guida di riferimento per la compilazione. Si precisa che alcuni dei contenuti richiesti potrebbero essere già definiti nel Sistema di Gestione Qualità del Fornitore. In questo caso il Piano della Qualità indicherà solo i riferimenti a tali procedure/processi, ecc. e descriverà solo le personalizzazioni specifiche.

Scopo e Campo di applicazione

Si chiede di indicare:

- la finalità del documento ed il suo campo di applicazione;
- gli eventuali allegati al piano della qualità.

Documenti applicabili e di riferimento

Documenti applicabili

Si chiede di indicare:

il Sistema di Gestione della Qualità (SGQ) usato per il contratto;

le certificazioni rilasciate al SGQ e la loro data di scadenza;

altri piani pertinenti (ad esempio i piani di progetto, piani di gestione ambientale, di salute e sicurezza sul lavoro, di sicurezza e di gestione delle informazioni).

Documenti di riferimento

Si chiede di indicare i documenti che costituiscono un riferimento per quanto esposto nel presente Piano della Qualità.

Glossario

Si chiede di descrivere abbreviazioni, acronimi, definizioni che sono utilizzate all'interno del Piano della Qualità.

Organizzazione

Si chiede di:

- definire l'organigramma del gruppo di lavoro impegnato sul contratto e le interfacce con Consip S.p.A. e con altri soggetti necessarie per l'esecuzione delle attività contrattuali (Ad esempio: Subfornitori, partner, autorità di regolamentazione, personale di altri progetti di sviluppo, personale di help desk);
- associare compiti e precise responsabilità a ciascun ruolo definito nell'organigramma;

  (matrice delle responsabilità),

- identificare i responsabili previsti per la fornitura, quali ad esempio :
  - servizi della fornitura;
  - controlli da svolgere;
  - gestione configurazione;
  - assicurazione qualità;
  - relazioni con le altre organizzazioni coinvolte nella fornitura;
  - comunicazione con Consip S.p.A..

Descrizione dei servizi

Per ogni servizio contrattuale si chiede:

- il flusso e la descrizione dei processi necessari ad erogare il servizio;
- le modalità di erogazione in situazioni normali ed in caso di problemi;
- le risorse (hardware, software, persone, ecc.) assegnate.

In alternativa si può inserire il riferimento ad eventuali procedure applicabili con l'indicazione di eventuali personalizzazioni.

Obiettivi qualità dei servizi della fornitura

Si chiede identificare, in modo chiaro e non ambiguo, i requisiti di qualità del contratto, eventualmente aggiornati con quanto proposto in offerta.

Per questo è necessario definire:

- gli attributi di qualità relativi a ciascun prodotto ed a ciascun servizio;
- gli indicatori di qualità con cui misurare gli attributi identificati;
- i valori limite ritenuti accettabili con cui confrontare le misure degli attributi di qualità.

Si chiede di descrivere le modalità che saranno utilizzate dal Fornitore per valutare la qualità dei prodotti e dei servizi realizzati (output del contratto) prima che tali prodotti e/o servizi vengano consegnati/erogati.

In particolare si chiede di esplicitare:

- modalità di misura o di rilevamento dei dati;
- modalità di calcolo e di aggregazione delle misure (per il computo di indicatori derivati);
- frequenza delle misure;
- periodi temporali di riferimento;
- le regole con cui si perviene ai giudizi di Approvazione Incondizionata/Approvazione con Riserva / Non Approvazione di un prodotto e/o un servizio considerando i risultati delle misure relative ai singoli attributi di qualità associati al prodotto.

5.7 Predisposizione dell'infrastruttura e dei servizi

Il Fornitore dovrà prevedere una pianificazione di dettaglio delle diverse fasi ed attività identificate.

Il piano di lavoro dovrà indicare in particolare le strategie e le tempistiche idonee a prevedere:

- tempi e caratteristiche di continuità, a parità di condizioni di qualità e di livello di servizio, dei servizi di connettività;
- descrizione dettagliata della migrazione, step by step, dei servizi ospitati nella attuale intranet Consip, verso il CS del Fornitore;
- definizione dei servizi base, in accordo con la Consip, che saranno i primi ad essere attivati in ragione dei dimensionamenti che si renderanno necessari al momento dell'avvio delle attività;
- tempi e caratteristiche di attivazione dei servizi totalmente esternalizzati (ex. protocollo informatico, posta elettronica, ecc.).

Il Fornitore entro il **termine massimo di 60 (sessanta) giorni solari dalla data di stipula del contratto**, ovvero dalla data di avvio dello specifico Ambito di servizio comunicata dalla Consip, dovrà aver completato le attività di:

- affiancamento allo scopo di acquisire conoscenza specifica sui contenuti dei vari Ambiti;

- formazione di start-up per tutti gli operatori necessari per la gestione delle PdL e per il personale di help desk di primo livello e per il personale di gestione degli apparati (server, firewall, rete Wi-Fi, ecc.) che saranno dislocati presso la sede Consip;
- attivazione dei servizi base in ragione dei dimensionamenti che si renderanno necessari al momento dell'avvio delle attività come definiti nel Piano di Migrazione;
- predisposizione dell'ambiente virtuale, come specificato nel capitolato, all'interno del CS del Fornitore atto ad ospitare gli applicativi Consip.

Il Fornitore dovrà dare avvio **a tutti i Servizi richiesti dal presente capitolato entro 90 (novanta) giorni solari** dalla data di stipula del contratto.

5.8 Collaudo tecnico funzionale

La totalità dei servizi offerti dal Fornitore (connettività e servizi in hosting) saranno sottoposti a collaudo da parte di personale Consip. Tale collaudo potrà interessare uno o più servizi compatibilmente con il Piano di Migrazione concordato. L'esecuzione del collaudo seguirà il piano di test predisposto dal Fornitore e condiviso con Consip. Si procederà ad un test funzionale dei servizi descritti nel presente capitolato, sottoponendo a collaudo anche le infrastrutture tecnologiche e le relative integrazioni laddove necessarie per supportare la realizzazione dei vari servizi necessari al funzionamento dell'infrastruttura.

Ai collaudi dovrà collaborare il Fornitore, che provvederà, con mezzi, materiali e personale specializzato proprio, a:

- supportare l'esecuzione dei test di collaudo del servizio;
- compilare il rapporto di collaudo, secondo il formato concordato con Consip, in cui sono tracciate tutte le attività eseguite nel corso del collaudo.

Nel caso di esito negativo del collaudo, in cui sia stata riscontrata una anomalia non bloccante, potrà essere eseguita una seconda prova entro un massimo di 3 giorni dalla data di completamento del test, risultante da apposito verbale. Nel caso in cui l'anomalia riscontrata sia di tipo bloccante potrà essere eseguita una seconda prova entro un massimo di 1 giorno dalla data del primo esito negativo di collaudo, risultante da apposito verbale.

In caso di esito negativo della seconda verifica di conformità si procederà secondo le indicazioni previste da contratto.

Qualora il collaudo risultasse positivo verrà redatto e sottoscritto da Consip il verbale di collaudo accettazione cui potrà essere allegato il documento rapporto di collaudo in cui sono tracciate le attività svolte durante il collaudo stesso.

Successivamente Consip comunicherà formalmente al Fornitore la "Data di inizio attività" per l'erogazione del Servizio.

5.9 Verifiche dei livelli di servizio e di conformità

I momenti di controllo e verifica del contratto sono costanti per tutta la durata della fornitura e garantiscono una visibilità completa e dettagliata dell'avanzamento delle attività.

Con cadenza mensile e comunque ogni volta si renda necessario su richiesta di Consip o del Fornitore verrà eseguita una verifica dell'andamento operativo della fornitura (SAL Operativo) con la finalità di monitorare le attività operative e gli SLA richiesti per i servizi. Gli attori coinvolti saranno i responsabili operativi di Consip e del Fornitore.

Il risultato della verifica sarà contenuto in un verbale di SAL.

Consip, inoltre, si riserva la facoltà di convocare in corso di esecuzione del contratto incontri con il Fornitore in, al fine di affrontare aspetti e/o criticità che necessitano di un confronto.

Tali momenti particolari di collaudo o verifica riguardano principalmente:

- Collaudo delle attività propedeutiche;
- Collaudo subentro dei servizi;
- Verifiche richieste nuove attivazioni;
- Verifiche prestazione dei servizi;
- Altre verifiche dei livelli di servizio;
- Audit qualità.

5.10 Revisione dei requisiti di qualità

Durante l'intero periodo contrattuale ciascun requisito di qualità potrà essere riesaminato su richiesta della Consip; il riesame potrà derivare da nuovi strumenti di misurazione non disponibili alla data di stipula del contratto e/o dall'adeguamento delle metodiche atte alla rilevazione dei singoli requisiti di qualità che sono risultate non efficaci.

Consip ed il Fornitore, in caso di necessità, concorderanno eventuali modifiche ai metodi di calcolo successivamente riportati.

Il Fornitore si impegna a erogare i servizi tenendo conto delle modifiche richieste da Consip e a recepirle nel Piano della Qualità.

Nella stesura del Piano della Qualità, che sarà sottoposto all'approvazione di Consip, il Fornitore per ciascun requisito di qualità dovrà dettagliare le fonti dati utilizzate per la raccolta dei dati elementari nonché gli strumenti per l'elaborazione delle informazioni di dettaglio.

Per la verifica del rispetto dei requisiti di qualità contrattuali il Fornitore si impegna a predisporre ed installare, senza alcun onere aggiuntivo per Consip e/o per l'Amministrazione, idonei strumenti di misura hardware e/o software e, ove non possibile, ad effettuare rilevazioni manuali dei parametri da misurare, entro la data di fine del periodo transitorio.

Tutti i dati rilevati e tutti quelli oggetto dei report periodici (mensili, trimestrali, ecc.) saranno archiviati a cura del Fornitore che ne dovrà garantire l'accessibilità alla Consip attraverso adeguati strumenti hw e sw. Inoltre il Fornitore si impegna a fornire la base dati

(RDBMS) di dettaglio, contenente tutti i dati rilevati, utilizzata per la valorizzazione dei requisiti di qualità secondo le modalità descritte nel Capitolato tecnico.

5.11 Audit qualità

Consip si riserva la facoltà di effettuare audit di qualità presso il Fornitore. Tali audit saranno finalizzati a monitorare e verificare che le attività e/o i processi siano svolti dal Fornitore nel rispetto di quanto definito a livello contrattuale.

Consip provvede ad organizzare l'audit, predisponendo eventuali check list di supporto, e si accorda con il Fornitore in merito alla data di svolgimento delle verifiche ispettive.

Consip esegue la verifica ispettiva e a conclusione della stessa redige il verbale di verifica annotando eventuali anomalie riscontrate.

Il verbale di verifica viene inviato da Consip al Fornitore affinché questi, in conseguenza di eventuali non conformità rilevate, ne individui le cause, definisca tempi e modi delle azioni da intraprendere; il Fornitore provvede successivamente ad inviare le proposte delle azioni correttive a Consip per verifica e approvazione.

Consip si riserva, inoltre, la facoltà di richiedere al Fornitore la definizione di azioni correttive, preventive o migliorative, ad esempio in relazione ad eventi notificati in sede di monitoraggio della fornitura o di gestione di rilievi e penali, al fine di incidere sulle cause che hanno generato l'evento notificato ed evitare il ripetersi o il verificarsi di un problema.

5.12 Audit sicurezza

Consip si riserva la facoltà di effettuare audit di sicurezza presso il Fornitore. Tali audit saranno finalizzati a monitorare e verificare che le attività e/o i processi siano svolti dal Fornitore nel rispetto di quanto definito a livello contrattuale.

In particolare, il fornitore deve:

- accettare visite ispettive da parte di Consip o da terze parti designate/incaricate;
- concordare con gli auditor il contenuto e la tempificazione delle eventuali azioni correttive, preventive, migliorative, porle in atto assicurandone il tracciamento fino alla verifica del buon fine ("chiusura") da parte degli auditor.

Da parte sua Consip si impegna a raccogliere e valutare motivate proposte migliorative, comunque sottoposte, per il possibile loro recepimento in successive versioni delle politiche di sicurezza.

In particolare, il fornitore è responsabile del corretto utilizzo e gestione, da parte del suo personale, delle credenziali che gli vengono rilasciate per l'accesso ai sistemi di Consip.

5.13 Chiusura della Fornitura

Il Fornitore è chiamato, al termine del rapporto contrattuale, a fornire il supporto per il subentro dell'eventuale nuovo gestore dei servizi.

Nei ultimi 3 mesi della durata del Contratto o nel caso di cessazione anticipata del rapporto contrattuale, il Fornitore dovrà effettuare verso Consip o terzi da essa designati, il trasferimento delle competenze sulle attività condotte, e il trasferimento dei dati ospitati presso il proprio CS al fine di rendere la prosecuzione delle attività quanto più agevole possibile.

In questo periodo Consip potrà terminare la fornitura in funzione delle attività di subentro messe in atto dal nuovo Fornitore secondo una modalità di passaggio graduale dei servizi.

In tale modo i servizi forniti dal Fornitore uscente potranno essere rilasciati, anche singolarmente. Si intende che Consip provvederà a dismettere i servizi del Fornitore uscente mano a mano che quelli del Fornitore entrante verranno collaudati.

La chiusura del contratto viene attestata dalla formalizzazione di un "Verbale di chiusura" verificato dal Direttore dell'Esecuzione del Contratto e dal Responsabile Operativo, approvato dal Responsabile di contratto di Consip, che attesta la completa migrazione dei servizi di rete e la chiusura delle attività di responsabilità del Fornitore.