ALLEGATO A

CAPITOLATO TECNICO E RELATIVE APPENDICI

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

CAPITOLATO TECNICO – PARTE GENERALE

PROCEDURA RISTRETTA, SUDDIVISA IN 4, LOTTI PER L'AFFIDAMENTO DEI SERVIZI DI *CLOUD COMPUTING*, DI SICUREZZA, DI REALIZZAZIONE DI PORTALI E SERVIZI ONLINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI (ID SIGEF 1403).

1. PREMESSA

Il presente Capitolato Tecnico ha lo scopo di descrivere i contenuti ed i requisiti minimi in termini di quantità, qualità e livelli di servizio relativi alla fornitura dei servizi cui deve riferirsi il Fornitore per la formulazione dell'Offerta Tecnica.
In particolare, oggetto della gara è la stipula, per ognuno dei 4 Lotti in cui essa è suddivisa, di un Contratto Quadro per l'affidamento dei servizi elencati nel seguito in favore delle Pubbliche Amministrazioni e che dovranno essere erogati nell'arco di cinque anni:

- Servizi Infrastrutturali per la PA (Servizi *Cloud* e di migrazione da fisico a virtuale);
- Identità digitale e sicurezza applicativa (IAM-Identity&Access Management e sicurezza applicativa);
- Interoperabilità per i dati (Open/Big Data) e cooperazione applicativa;
- Portali e Servizi on-line (portali, App mobile, gestione dei contenuti).

Nel presente Capitolato Tecnico le caratteristiche minime e i requisiti minimi, nonché le previsioni ove il Fornitore o l'offerta è previsto che "deve obbligatoriamente" ovvero "dovranno obbligatoriamente", sono da intendersi obbligatori e vincolanti, da possedere quindi a pena di esclusione.
La **"giornata"** o i **"giorni"** vanno intesi come solari, salvo ove diversamente specificato.
Il Fornitore potrà proporre, in sede di offerta tecnica, migliorie relativamente ai servizi oggetto di fornitura che, in caso di aggiudicazione, diverranno vincolanti per l'erogazione degli stessi e che saranno oggetto di valutazione in sede di procedura.

1.1. Acronimi

AgID: Agenzia per Italia Digitale
API: Application Programming Interface
BI: Business Intelligence
CAD: Codice dell'Amministrazione Digitale
CONSIP: Consip S.p.A.
F/OSS: Free and Open Source Software
IaaS: Infrastructure as a Service
ICT: Information and Communication Technology
IDS: Intrusion Detection Systems
IE: Internet Explorer
IPS: Intrusion Prevention Systems
IT: Information Technology
KPI: Key Performance Indicator
PA: Pubblica Amministrazione
PAC: Pubblica Amministrazione Centrale
PAL: Pubblica Amministrazione Locale
PaaS: Platform as a Service
SaaS: Software as a Service
SPCoop: Sistema Pubblico di Connettività e Cooperazione
HTTP: Hyper Text Transport Protocol
HTTPS: Secure HyperText Markup Language
IMAP: Internet Mail Access Protocol
QXN: Qualified eXchange Network
SMTP: Simple Mail Transfer Protocol
SAL: Stato Avanzamento Lavori
SAN: Storage Area Network
SGSI: Sistema di Gestione della Sicurezza delle Informazioni
SPC: Sistema Pubblico di Connettività
VDC: Virtual Data Center
VLB: Virtual Load Balancer
VM: Virtual Machine
VNetwork: Virtual Network
VF: Virtual Firewall (VF)
VTS: Virtual Traffic Shaper (VF)
VPN: Virtual Private Network

V-DNS: Virtual Domain Name System

1.2. Definizioni

Aggiudicatario/Fornitore: va intesa l'Impresa/RTI aggiudicataria della fornitura; se non diversamente indicato va inteso l'aggiudicatario di ciascuno dei Lotti della fornitura
Amministrazioni: Pubbliche Amministrazioni
Amministrazione aggiudicatrice: Consip.
Amministrazione/i Contraente/i: Pubbliche Amministrazioni che hanno siglato un Contratto di Fornitura con il Fornitore per l'erogazione di uno dei servizi in ambito dell'Accordo Quadro
Modalità "*As a Service*": Servizio erogato da remoto attraverso i Centri Servizi
Modalità "*On premise*": Servizio erogato presso le strutture dell'Amministrazione contraente o altre strutture indicate dalla stessa.
Fornitore Lotto 1: va inteso il concorrente aggiudicatario del Lotto 1
Fornitore Lotto 2: va inteso il concorrente aggiudicatario del Lotto 2
Fornitore Lotto 3: va inteso il concorrente aggiudicatario del Lotto 3
Fornitore Lotto 4: va inteso il concorrente aggiudicatario del Lotto 4

2. CONTESTO

2.1. Contesto di riferimento

Negli ultimi 10 anni il Legislatore ha diretto la propria attenzione alla digitalizzazione dei rapporti tra cittadini/imprese e Pubblica Amministrazione, dando vita ad un insieme di norme che sviluppano il progetto della Pubblica Amministrazione Digitale.
La prima importante azione riformatrice in tale direzione è stata l'emanazione del D.lgs. 82/2005 e s.m.i. - cosiddetto Codice dell'Amministrazione Digitale (CAD) - che ha individuato le strategie organizzative e tecnologiche per accrescere la digitalizzazione della P.A. italiana, dettando per la prima volta alle Amministrazioni obblighi, responsabilità e scadenze per l'attuazione degli specifici interventi in materia di innovazione.
La riforma digitale si propone il perseguimento dei seguenti obiettivi:

- offrire ai cittadini servizi innovativi e di qualità, monitorandone il livello di soddisfazione;
- dare pieno valore giuridico alla transazioni digitali tra cittadini e Pubblica Amministrazione;
- permettere la tracciabilità dello stato di una pratica in tempo reale e la consegna/ricezione telematica della documentazione, con la conseguente eliminazione delle code agli sportelli e della consegna di documentazione già in possesso della P.A.;
- rendere trasparente e facilmente fruibile il rapporto tra cittadini e imprese con le PP.AA., fornendo agli utenti un alto grado di informazioni sui servizi resi dall'Amministrazione e le modalità per accedervi;
- rendere disponibili, ai cittadini e alle altre Amministrazioni, i dati raccolti, prodotti e gestiti da una Amministrazione, permettendo la loro valorizzazione;
- creare una Amministrazione pienamente interoperabile e cooperativa, in cui i servizi sviluppati da una Amministrazione sono ottimizzati dalla cooperazione con i servizi di altre Amministrazioni.

Il CAD individua le seguenti azioni (con relativi obblighi, responsabilità e scadenze) che ogni Amministrazione deve intraprendere per il raggiungimento degli obiettivi sopra declinati:

- obbligo di dotarsi degli strumenti necessari alla gestione dei procedimenti amministrativi attraverso le tecnologie dell'innovazione, raccogliendo tutti i dati e i documenti facenti capo a un medesimo procedimento in un "fascicolo informatico" che dovrà essere facilmente accessibile dal cittadino;
- identificazione informatica univoca e sicura del cittadino/impresa che accede a servizi on-line della Pubblica Amministrazione;

- accettazione di istanze e dichiarazioni presentate per via telematica alle Pubbliche Amministrazioni sottoscritte mediante la firma digitale;
- interoperabilità dei sistemi e integrazione dei processi di servizio fra le diverse Amministrazioni nel rispetto delle regole tecniche della Cooperazione Applicativa SPC;
- realizzazione degli scambi di documenti informatici tra le Pubbliche Amministrazioni attraverso la cooperazione applicativa nell'ambito del SPC, nel rispetto delle relative procedure e regole tecniche di sicurezza, che costituiscono invio documentale valido ad ogni effetto di legge;
- obbligo a rendere disponibili in formato aperto e accessibile tutti i dati pubblici prodotti e gestiti;
- realizzazione dei siti istituzionali secondo i principi dell'accessibilità, dell'usabilità, della reperibilità e della completezza delle informazioni e dei servizi in essi contenuti. Il sito dovrà obbligatoriamente contenere tutte le informazioni per comunicare con la P.A., tra cui almeno un indirizzo di posta elettronica certificata, l'elenco dei servizi on-line messi a disposizione, l'elenco dei documenti e i moduli richiesti per ogni procedimento.

Altro passo fondamentale è stato l'istituzione dell'Agenda Digitale Italiana, volta a recepire le direttive dell'Agenda Digitale Europea, avvenuta il 1 marzo 2012 con decreto del Ministro dello sviluppo economico, di concerto con il Ministro per la Pubblica Amministrazione e la semplificazione, il Ministro per la coesione territoriale, il Ministro dell'istruzione, dell'università e della ricerca e il Ministro dell'economia e delle finanze. L'Agenda Digitale Italiana consta di una serie di norme, provvedimenti, linee di azione e strategie volti a realizzare i cosiddetti 6 pilastri dell'Agenda:

- infrastrutture e sicurezza: i principali interventi previsti sono sul piano della "banda larga" e "ultralarga", il cui obiettivo è quello di garantire ai cittadini l'accesso a internet veloce e superveloce e ad applicazioni interoperabili, garantendo l'accesso a velocità superiori a 30 Mbps entro il 2020 garantendo contemporaneamente elevati standard di qualità e sicurezza. Altro obiettivo importante è la realizzazione in modalità *cloud computing* dei Data Center della Pubblica Amministrazione, al fine di ottimizzare le risorse tecnologiche e rendere i sistemi interoperabili e riusabili;
- e-commerce;
- e-government: obiettivo primario è quello di realizzare la rivoluzione digitale della Pubblica Amministrazione, attraverso una serie di norme che agiscano sulla digitalizzazione delle tre grandi aree tematiche della Pubblica Amministrazione:

- affari interni, con l'istituzione del domicilio digitale del cittadino e l'evoluzione dell'Indice Nazionale delle Anagrafi in una rete interoperabile dei dati anagrafici gestiti dai vari organi pubblici;
- giustizia digitale, con l'introduzione di comunicazioni e notifiche telematiche, obbligatorietà per gli avvocati di comunicare il proprio indirizzo PEC nei ricorsi e negli atti difensivi, la realizzazione del processo civile telematico che rappresenta la trasformazione innovativa dell'intero impianto giudiziario;
- sanità digitale, con la digitalizzazione dei processi sanitari come la trasmissione telematica dei certificati di malattia dei dipendenti pubblici e privati, la realizzazione del fascicolo sanitario elettronico, la digitalizzazione dei referti medici e delle cartelle cliniche.

Altri interventi necessari alla digitalizzazione della P.A. sono individuati negli obblighi sulla fatturazione elettronica e gli open data;

- competenze digitali;
- ricerca e innovazione;
- smart communities.

Il 18 ottobre 2012 è stato pubblicato in Gazzetta Ufficiale il Decreto Legge n° 179 recante "Ulteriori misure urgenti per la crescita del Paese" - c.d. provvedimento Crescita 2.0 – che ha individuato le priorità e le modalità di attuazione dell'Agenda Digitale Italiana e aggiornato lo stesso Codice per l'Amministrazione Digitale allineandolo agli obiettivi dell'Agenda Digitale.

In tale scenario normativo è nata l'esigenza di fornire alle Pubbliche Amministrazioni dei servizi innovativi finalizzati al raggiungimento degli obblighi di legge stabiliti dal Codice per l'Amministrazione Digitale e all'attuazione dell'Agenda Digitale Italiana.
A tal fine Consip S.p.A. ha bandito, ai sensi e per gli effetti dell'art.4, comma 3-quater, del D.L. n. 95/2012, convertito con modificazioni in L. n. 135/2012, dell'art.20, comma 4, del D.L. n. 83/2012, convertito con modificazioni in L. n. 134/2012 e ai sensi dell'art. 1, comma 192, della Legge n. 311/2004, la presente procedura di gara per i servizi di *Cloud Computing*, di Sicurezza, di Realizzazione di Portali e Servizi on-line e di Cooperazione Applicativa per le Pubbliche Amministrazioni, suddivisa in quattro lotti.

2.2. Obiettivi ed evoluzione

L'iniziativa in oggetto si pone un duplice obiettivo:

- da un lato quello di garantire l'evoluzione dei servizi già previsti nelle precedenti inziative SPC, con particolare riferimento alla gara a procedura ristretta n. 1/2006, comprensiva di servizi di progettazione, realizzazione e gestione di servizi di siti web e conduzione sistemi (Lotto 1) e di servizi di interoperabilità evoluta e cooperazione e sicurezza applicativa (Lotto 2) in favore delle Pubbliche Amministrazioni, nell'ambito del Sistema pubblico di connettività;
- dall'altro lato, la presente iniziativa ha l'obiettivo di rendere disponibili alle Amministrazioni Pubbliche italiane servizi innovativi di carattere abilitante per la realizzazione dell'Agenda Digitale Italiana.

Ad esempio, i servizi di *cloud computing*, compresi nel Lotto 1 della presente iniziativa, favoriranno il consolidamento dei CED delle Pubbliche Amministrazioni, attraverso servizi abilitanti quali la migrazione "da fisico a virtuale" dei CED della PA e la fruizione di software, piattaforme e hardware in logica *cloud* (SaaS, PaaS, IaaS) su infrastrutture centralizzate. Di pari passo con il consolidamento dei CED, l'iniziativa mira a diffondere – rendendone più agevole l'acquisizione da parte delle Amministrazioni contraenti – servizi che supportino le normali attività istituzionali a più livelli, sia in termini di erogazione verso l'utenza secondo nuovi paradigmi (es. portali web di nuova generazione e "App" fruibili attraverso i dispositivi mobili), sia in termini di efficientamento dei processi interni, con particolare riguardo a quelle soluzioni e quegli strumenti in grado di garantire cooperazione tra le Amministrazioni (es. cooperazione applicativa, open data) e maggiore capacità di *intelligence* sul patrimonio informativo della PA (es. attraverso i servizi di Big Data), finalizzata ad esempio al contrasto alle frodi o al miglioramento dei servizi resi ai cittadini.

I servizi di gestione dell'dentità digitale favoriranno la diffusione dei servizi telematici, sia nelle transazioni tra soggetti privati e imprese che nell'interazione tra le Pubbliche Amministrazioni ed i cittadini. Il servizio è essenzialmente concepito per agevolare la migrazione delle identità digitali attualmente gestite dalle amministrazioni verso un identity provider esterno con il quale si è stabilita una relazione di fiducia (trust) nell'ottica della realizzazione di una gestione federata delle identità.

L'importanza di questa tematica ha avuto giusto riconoscimento sul piano normativo dal DL 69 del 21/6/2013 che all'articolo 17-ter istituisce un sistema per la gestione delle identità digitali - denominato SPID - valido ai sensi di legge nell'ambito pubblico e privato.

Attraverso questa iniziativa di gara, quindi, si vogliono pertanto rendere disponibili servizi innovativi, o servizi tradizionali erogati in modalità innovativa, per favorire la PA nella sua graduale transizione verso l'era tecnologica "digitale".

2.3. Il ruolo di AGID

Nel contesto normativo definito nel presente documento, opera l'Agenzia per l'Italia Digitale (AgID), istituita ai sensi dell'articolo 19 del D.L. del 22 giugno 2012, n. 83, convertito in legge, con modificazioni, dall'art. 1 della legge 7 agosto 2012, n. 134, e s.m.i., e preposta alla realizzazione degli obiettivi dell'Agenda digitale italiana.
L'Agenzia per l'Italia Digitale, nell'ambito delle funzioni attribuitele dalla normativa, relativamente ai servizi della presente procedura di gara, svolge le seguenti attività:

- detta indirizzi, regole tecniche, linee guida e metodologie progettuali in materia di sicurezza informatica, procedure e standard, anche di tipo aperto, con lo scopo di assicurare piena interoperabilità e cooperazione applicativa tra i sistemi informatici delle Amministrazioni;
- svolge attività di progettazione e coordinamento delle iniziative strategiche e di preminente interesse nazionale, anche a carattere intersettoriale, per la più efficace erogazione di servizi in rete della Pubblica Amministrazione a cittadini e imprese;
- elabora le linee guida finalizzate al consolidamento delle infrastrutture digitali delle Pubbliche Amministrazioni, alla razionalizzazione dei relativi CED e migrazione al modello del *cloud computing* coerentemente con gli obiettivi dell'Agenda Digitale;
- vigila sulla qualità dei servizi e sulla ottimizzazione della spesa in materia informatica, anche in collaborazione con Consip S.p.A. e SOGEI S.p.A..

2.4. Il ruolo dei comitati di governo

La presente fornitura prevede la costituzione di organismi di controllo e governo, deputati alla direzione tecnica del Contratto Quadro di ogni Lotto.
Per ogni Lotto, quindi, sarà costituito, successivamente alla sottoscrizione del Contratto Quadro, un **Comitato di Direzione Tecnica** (di seguito Comitato), formato da due Referenti Consip/AgID e da due Rappresentanti del Fornitore.
Quando richiesto dai temi all'ordine del giorno, al Comitato potrà partecipare un Referente delle Amministrazioni contraenti coinvolte o soggetti terzi indicati da AgID/Consip/Fornitore aggiudicatario.
Le funzioni di Presidente e di Segretario saranno svolte dai Referenti Consip/AgID.

Il Comitato si riunirà su convocazione del Presidente, che avverrà a mezzo PEC con almeno 5 (cinque) giorni solari di preavviso.

Il Fornitore assume l'obbligo di fornire al Comitato di Direzione Tecnica, con cadenza almeno annuale, un documento che illustri l'evoluzione tecnologica sul mercato dei servizi oggetto del proprio contratto con eventuali proposte di adeguamento dei servizi stessi (cfr. par. 6.4).

Il Comitato di Direzione Tecnica svolgerà le seguenti funzioni:

1. supervisione del funzionamento complessivo dei servizi previsti nel Contratto Quadro e valutazione, con periodicità annuale, dell'adeguatezza delle disposizioni del Contratto Quadro ed eventuale formulazione di proposte di emendamento da sottoporre alle parti;
2. verifica, con periodicità trimestrale, dello stato di avanzamento del Contratto Quadro;
3. facoltà di modificare le modalità di esecuzione della fornitura, di introdurre nuove modalità, di definire/modificare gli attuali standard, anche in corso d'opera.
4. verifica con periodicità trimestrale dei Livelli di Servizio;
5. riesamina i livelli di servizio; 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 indicatori di qualità che sono risultate non efficaci.
6. proposta di inserimento di nuovi prodotti/servizi, complementari ai servizi già oggetto della presente fornitura nel rispetto dei massimali contrattuali, che potranno essere resi dal Fornitore alle Amministrazioni;
7. proposta dei prezzi dei nuovi servizi di cui al precedente punto;
8. approvazione della revisione dei prezzi come da procedura definita nel capitolo 8 del presente documento.

Inoltre, il Comitato di Direzione Tecnica potrà eseguire:

a) verifica della rispondenza del Progetto dei Fabbisogni (rif. Cap. 7) secondo quanto disposto nel Capitolato Tecnico;
b) esame del Progetto dei Fabbisogni di servizi su richiesta dell'Amministrazione interessata;
c) esame degli interventi di manutenzione programmata che comportino l'interruzione della fornitura dei servizi;

3. DEFINIZIONE DELLA FORNITURA

I servizi oggetto di fornitura della presente iniziativa sono riservati alle Pubbliche Amministrazioni interconnesse direttamente alla rete SPC (o altre strutture equivalenti individuate da Consip/Agid) attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati.
La fornitura è costituita dall'insieme di servizi elementari descritti nei successivi paragrafi.

3.1. Oggetto

Il presente Capitolato Tecnico descrive i contenuti e i requisiti minimi relativi alla erogazione di servizi, sulla base della suddivisione in Lotti di seguito descritta:

- Lotto 1 - Servizi di *cloud computing*,
- Lotto 2 - Servizi di gestione delle identità digitali e sicurezza applicativa,
- Lotto 3 - Servizi di interoperabilità per i dati e di cooperazione applicativa,
- Lotto 4 - Servizi di realizzazione e gestione di Portali e Servizi on-line.

In particolare, la procedura per l'affidamento dei predetti servizi è articolata attraverso la stipula da parte di Consip S.p.A. di un Contratto Quadro con l'Aggiudicatario di ciascun Lotto, in modo del tutto disgiunto tra i singoli Lotti. Ciascun Aggiudicatario si impegna a stipulare, con le singole Amministrazioni contraenti, Contratti di Fornitura aventi ad oggetto i predetti servizi alle condizioni stabilite nel Contratto Quadro.
Si evidenzia altresì che tutti i servizi erogati in modalità da remoto (*as a service*) richiedono l'esecuzione attraverso Centri Servizi oggetto di certificazione ISO 27001 ed i cui requisiti sono descritti nel seguito del Capitolato Tecnico.
I servizi della presente fornitura dovranno essere erogati nel rispetto delle linee guida di riferimento definite da AgID e alle loro successive evoluzioni.

3.1.1. Lotto 1 – Servizi di *cloud computing*

Il Lotto 1 della presente fornitura comprende servizi in modalità *cloud computing* (IaaS, PaaS, SaaS) e servizi di abilitazione al *cloud*:

- *Servizi di calcolo e memorizzazione (Infrastructure as a Service - IaaS*) per la fruizione di risorse remote virtuali; le risorse remote virtuali sono rese disponibili per il tramite di risorse fisiche predisposte dal fornitore ad uso esclusivo delle Amministrazioni (*Community Cloud*). Tali servizi sono corredati da strumenti di gestione e configurazione e includono funzionalità di *networking* tra cui *virtual load balancer, virtual firewall*, *virtual lan*.

- *Servizi di tipo Platform as a Service (PaaS*) per la erogazione alle Pubbliche Amministrazioni di servizi *middleware* per lo sviluppo, collaudo, manutenzione ed esercizio di applicazioni. I servizi PaaS sono quindi identificati attraverso una o più architetture di servizi *software* (*Solution Stack*) che poggiano su un'infrastruttura di tipo *IaaS*. Le tipologie di *Solution Stack* si diversificano in funzione della tipologia di servizio applicativo che viene erogato. Tali servizi sono corredati da strumenti di gestione e di configurazione.
- *Servizi di tipo Software as a Service (SaaS)* per la erogazione di servizi applicativi alle Pubbliche Amministrazioni tra i quali servizi per la conservazione dei documenti (in conformità con gli artt. 43, 44 e 44-bis del CAD), servizi di collaborazione, servizi di produttività individuale, servizi di comunicazione unificata, servizi di analisi dei dati e reportistica. Tali servizi sono corredati da strumenti di gestione e configurazione. L'erogazione potrà avvenire anche attraverso la presa in carico da parte del Fornitore di prodotti/applicazioni individuati da AgID/Consip e realizzati nel rispetto delle regole tecniche derivanti dal CAD, ed in particolare delle Linee Guida sul Riuso pubblicate da AgID;
- *Servizi di Cloud Enabling*, tra cui il supporto alla virtualizzazione di infrastrutture fisiche nell'ambito dei CED privati delle Pubbliche Amministrazioni (migrazione *Phisical to Virtual*).

I servizi del Lotto 1 possono essere acquistati dalle Amministrazioni con l'obiettivo di:

1. migrare in modalità *cloud computing* il proprio Data Center, realizzando gli obiettivi dell'Agenda Digitale Italiana in materia di razionalizzazione dei Data Center e ottimizzazione delle infrastrutture;
2. creare servizi pubblici innovativi ad alto valore aggiunto e cooperabili con altri servizi di altre Amministrazioni;
3. ottemperare agli artt. 43, 44 e 44-bis del CAD sulla conservazione dei documenti informatici.

3.1.2. Lotto 2 – Servizi di gestione delle identità digitali e sicurezza applicativa

Il Lotto 2 della presente fornitura comprende le seguenti tipologie di servizi:

- *Servizi per la gestione delle identità digitali,* erogati in modalità *as a service*, in conformità anche all'art. 64 del CAD;
- *Servizi di firma digitale remota comprensiva della fornitura di certificati e di timbro elettronico*, erogati in modalità *as a service*, volti a favorire la dematerializzazione dei documenti e la digitalizzazione dei processi amministrativi;
- *Servizi di sicurezza*, erogati sia in modalità *as a service* che in modalità *on premise*, atti a garantire la sicurezza applicativa e a supportare le Amministrazioni nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità dei sistemi informativi; i servizi di sicurezza includono anche servizi professionali a supporto delle attività delle Unità Locali di Sicurezza o strutture equivalenti delle Pubbliche Amministrazioni.

Tali servizi possono essere utilizzati dalle Amministrazioni per:

1. ottemperare agli obblighi previsti in materia di gestione degli accessi ai servizi erogati in rete, anche in conformità all'art. 64 del CAD;
2. raggiungere l'obiettivo di diffusione dell'utilizzo della firma digitale nella P.A. e conseguentemente quello della diffusione del documento informatico sottoscritto con firma digitale;
3. ottemperare alla disposizioni in materia di "sicurezza dei dati, dei sistemi e delle infrastrutture delle Pubbliche Amministrazioni" previste dall'art. 51 del CAD;
4. realizzare gli obiettivi in materia di sicurezza previsti nell'Agenda Digitale.

3.1.3. Lotto 3 – Servizi di interoperabilità per i dati e di cooperazione applicativa

Il Lotto 3 della presente fornitura prevede:

- *Servizi di interoperabilità per i dati* finalizzati a garantire l'integrazione dei dati e dei metadati, la gestione di dati di tipo aperto, nonché la gestione dei Big Data;
- *Servizi di cooperazione applicativa*, preposti a favorire lo scambio di dati e informazioni fra le Pubbliche Amministrazioni garantendo l'integrazione dei procedimenti amministrativi delle stesse secondo le previsioni del CAD.

Tali servizi permettono alle Amministrazioni di:

1. realizzare gli obiettivi dell'Agenda Digitale sull'Amministrazione interoperabile e pienamente cooperativa;
2. ottemperare all'art. 52 del CAD in materia di valorizzazione del patrimonio informativo pubblico;
3. garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi in maniera conforme alle regole tecniche del sistema pubblico di connettività in materia di cooperazione applicativa e ottemperare all'art. 63 del CAD sulla cooperazione dei sistemi e dei procedimenti ;
4. ottemperare all'art. 12 del CAD in materia di utilizzo delle tecnologie ICT nell'azione amministrativa.

3.1.4. Lotto 4 – Servizi di realizzazione e gestione di Portali e Servizi on-line

Il Lotto 4 della presente fornitura prevede i seguenti macroambiti di servizio:

- *Servizi di realizzazione e gestione di Portali e Siti Web in logica di multicanalità,* che consentano all'Amministrazione contraente di sviluppare o evolvere i propri siti o portali, anche in versione *mobile,* eventualmente re-ingegnerizzandoli, o di rendere accessibili via web applicazioni interne pre-esistenti, gestendone anche la manutenzione correttiva ed adeguativa e la conduzione in esercizio, mediante servizi di Conduzione Applicativa, Gestione Operativa e Supporto Specialistico.
- *Servizi di gestione dei contenuti tramite soluzioni di "Content Management" erogate in modalità "as-a-Service" o tramite soluzioni "on premise" messe a disposizione dalle Amministrazioni;*
- *Servizi di realizzazione e gestione di "Apps" per dispositivi mobili,* che consentano all'Amministrazione committente di sviluppare o evolvere le proprie applicazioni per dispositivi mobili (es. smartphone e tablet), non solo per ciò che attiene alla componente *client* che ne consente l'utilizzo da parte degli utenti dai propri *device*, ma anche della componente di *back-end* necessaria al funzionamento dei servizi erogati dal *client*, gestendone anche la manutenzione correttiva ed adeguativa e la conduzione in esercizio, mediante servizi di Conduzione Applicativa, Gestione Operativa e Supporto Specialistico.

Attraverso l'utilizzo di tali servizi le Amministrazioni possono:

1. rispettare le prescrizioni di cui agli artt. 53 e 54 del CAD in merito a caratteristiche e contenuti dei siti istituzionali;
2. realizzare gli obiettivi dell'Agenda Digitale relativi all'e-government;
3. realizzare servizi innovativi per cittadini e imprese che permettano all'Amministrazione di interfacciarsi col cittadino anche attraverso i nuovi canali digitali.

3.2. Durata

Con riferimento a ciascun Lotto, la durata dei Contratto Quadro è fissata in:

- per il solo Lotto 1: 36 mesi prorogabili, su comunicazione di Consip, sino ad un massimo di ulteriori 24 mesi;
- per i Lotti 2, 3 e 4: 60 mesi;

in ogni caso a decorrere dalla stipula del Contratto Quadro medesimo, come meglio specificato nella Lettera di invito.

I singoli Contratti Esecutivi di Fornitura di ciascun Lotto avranno una durata decorrente dalla data di stipula del Contratto Esecutivo medesimo e sino al massimo della scadenza ultima, eventualmente prorogata (Lotto 1) del Contratto Quadro.

Le singole Amministrazioni contraenti potranno richiedere una proroga temporale dei singoli Contratti Esecutivi di Fornitura al solo fine di consentire la migrazione dei servizi ad un nuovo Fornitore al termine del Contratto Quadro, qualora la selezione dell'Operatore Economico subentrante non sia intervenuta entro i 3 mesi antecedenti la scadenza del presente Contratto Quadro.

Le durate delle eventuali proroghe dovranno essere modulate sulla base dello slittamento temporale misurato nella selezione dell'Operatore Economico subentrante, rispetto ai 3 mesi previsti per la migrazione dei servizi, ed avere una durata massima complessiva di 6 mesi.

Si precisa inoltre, facendo riferimento al successivo §7.2 per la modalità di erogazione prevista per i servizi oggetto di fornitura, che:

- per i servizi con modalità di erogazione "progettuale":
  - la durata del Contratto Esecutivo coincide con la durata prevista del progetto/attività e non potrà, in ogni caso, prolungarsi oltre la durata del Contratto Quadro;
- per i servizi con modalità di erogazione "continuativa":
  - la durata non può prolungarsi oltre il termine della durata massima del Contratto Quadro;
  - la finestra d'ordine del servizio, per ciascun lotto, termina in considerazione della durata minima di ciascun singolo servizio come stabilita nei capitolati

tecnici Lotto 1, 2, 3 e 4. Oltre tale termine, è facoltà del Fornitore accettare l'esecuzione dei servizi anche per durate inferiori, alle medesime condizioni contrattuali (considerando il rateo della periodicità offerta).

3.3. Normativa di riferimento

Si riportano nel presente paragrafo i riferimenti in termini di normativa e standard internazionali:

- Art. 615 Codice Penale – Accesso abusivo a un sistema informatico o telematico;
- Raccomandazione CE n. 89/9 –lista minima e lista facoltativa in materia di reati informatici;
- Legge 22 aprile 1941 n. 633 - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio ed integrata dal D.L.vo 29 dicembre 1992 n. 518 e D.L.vo 6 maggio 1999 n. 169;
- D.P.C.M. 15 febbraio 1989 - Coordinamento delle iniziative e pianificazioni degli investimenti in materia di automazione nelle amministrazioni pubbliche;
- Legge 23 dicembre 1993 n. 547 - Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica;
- D.L.vo 29/12/92 n.518 - pirateria di software (in attuazione della direttiva 91/250/CE – tutela giuridica dei programmi per elaboratore);
- L. 489/93 e 549/95 – registrazione dati;Decreto legislativo 6 maggio 1999, n. 169 - Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati;
- Direttiva 95/46/CE del Parlamento Europeo e del Consiglio;
- L. 626/96 e L. 242/96 – Sicurezza sul lavoro;
- L. 59/97 – trasmissione dati;
- L. 169/99 – tutela banche dati;
- L. 513/97 e DPCM/99 – firma digitale;
- Linee guida per la definizione di un Piano della sicurezza (AIPA - ottobre 1999);
- il Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 e successive modifiche);
- D.lgs 231/2001 – Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica;
- D.L.vo 28/12/2001 n. 467 norme penali a tutela della riservatezza dei dati personali

- Direttiva del P.C.M. del 16 gennaio 2002, pubblicata sulla G.U. n°69 del 22 marzo 2002 "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali";
- D.lgs 196/2003 – Codice in materia di protezione dei dati personali;
- Decreto legislativo 7 marzo 2005, n. 82 – "Codice dell'Amministrazione Digitale" con le modifiche ed integrazioni introdotte da DLGS 30 dicembre 2010 n. 235;
- Provvedimento del 27 novembre 2008 (G.U. 300 del 24/12/2008) "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- DCPM del 3 dicembre 2013 in materia di sistema di conservazione e successiva circolare dell'Agenzia per l'Italia Digitale n. 65/2014 (G.U. n. 89 del 16/04/2014) che abroga la precedente circolare di DigitPA n. 59 del 2011;
- UNI EN ISO 19011:2003 – Linee guida per gli audit dei sistemi di gestione;
- ISO/IEC 27001:2005 – Information security management systems – Requirements;
- ISO/IEC 27002:2005 – Code of practice for information security management;
- ISO/IEC 27005:2008 – Information security risk management;
- BS25999-2:2007 – Business continuity management – Specification;
- BS25777:2008 – Information and communications technology continuity management, Code of practice;
- COBIT v4.1 – Control Objectives for Information and related Technologies;
- ITIL v.3 2011 – Information Technology Infrastructure Library;
- Eventuali successive modificazioni delle norme e standard di riferimento;
- Ogni altra disposizione normativa e regolamentare applicabile.

Si precisa inoltre che la proprietà intellettuale dei dati e delle configurazioni necessarie all'utilizzo o frutto dell'utilizzo dei servizi oggetto della presente fornitura restano di proprietà dell'Aministrazione contraente.

4. DESCRIZIONE DEI CENTRI SERVIZI

L'erogazione dei servizi in modalità *as a service*, indicati nel presente Capitolato, richiede che il Fornitore dovrà disporre obbligatoriamente di Centri Servizi.

4.1. Requisiti del Centro Servizi

Il Fornitore dovrà descrivere dettagliatamente nell'offerta progettuale le soluzioni adottate per Centri Servizi , che devono obbligatoriamente rispondere a tutti i requisiti indicati nel Capitolo 4 e di seguito descritti.
Consip/AgID si riservano la possibilità di eseguire un collaudo dei Centri Servizi secondo le modalità esplicitate nel § 7.2.6.2.

4.1.1. Sede

I Centri Servizi in cui l'Aggiudicatario erogherà i servizi di cui al presente Capitolato dovranno essere obbligatoriamente dislocati su sedi ubicate sul territorio comunitario ed ottemperare la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio. È fatto obbligo inoltre al Fornitore di trattare, trasferire e conservare le eventuali repliche dei dati conservati dai suddetti Centri Servizi, ove autorizzate dalle Amministrazioni, sempre all'interno del territorio comunitario; tali repliche dei dati dovranno essere conservate con livelli di sicurezza concordati con le Amministrazioni richiedenti.
Ciascun Centro Servizi – inteso come la struttura complessiva all'interno della quale è ritagliata dal Fornitore l'infrastruttura dedicata alle Amministrazioni contraenti - ed il personale ad esso addetto potranno non essere esclusivamente dedicati alla erogazione dei servizi di cui al presente Capitolato ma dovranno, comunque, rispettare i requisiti di cui al presente capitolato.
Si richiede che il Fornitore indichi l'ubicazione dei Centri Servizi e le principali caratteristiche in termini di logistica e condizioni ambientali (es. almeno: infrastrutture di collegamento, impianto elettrico, dislocazione apparecchiature di rete e server, illuminazione, sicurezza, insonorizzazione, aerazione e impianto di climatizzazione artificiale).
Per quanto attiene più in particolare all'infrastruttura utilizzata dal Fornitore ai fini dell'erogazione dei servizi oggetto della presente fornitura, si precisa che il/i CED e le relative macchine fisiche potranno essere condivisi esclusivamente con altre i Pubbliche Amministrazioni (PAC e PAL o altre Amministrazioni), in logica di *Community Cloud*; resta in ogni caso inteso che il Fornitore dovrà garantire ad ogni singola

Amministrazione contraente la segregazione logica degli ambienti e dei dati (ad esempio attraverso macchine virtuali e VLAN dedicate).

4.1.2. Responsabilità

L'Aggiudicatario nell'ambito della Fornitura deve nominare, nei termini previsti nello Schema di Contratto Quadro, un Responsabile dei Centri Servizi che avrà il compito di coordinare tutte le attività necessarie alla erogazione dei servizi previsti, ivi comprese quelle relative alla sicurezza.

L'Aggiudicatario deve nominare, nei termini previsti nell'Allegato 4A - Schema di Contratto Quadro, singoli responsabili per ognuna delle Amministrazioni contraenti (per ordini di singolo servizio o gruppi di servizi contenuti nel presente Capitolato) che avranno il compito di:

- coordinare le attività relative alla erogazione del singolo servizio;
- gestire i rapporti operativi con la singola Amministrazione contraente.

4.1.3. Infrastruttura tecnologica

L'infrastruttura tecnologica dei Centri Servizi dovrà garantire elevati livelli di integrazione, scalabilità, performance e resilienza.

I Centri Servizi dovranno garantire la continuità di servizio, per ciascun lotto e per ciascun servizio erogato in remoto, in coerenza con gli orari di servizio (cfr. Cap. 9) e con gli Indicatori di Qualità. In caso di eventi di disastro che rendono indisponibile l'intero sito preposto all'erogazione dei servizi remoti il fornitore dovrà invocare formalmente verso AGID/Consip tale evento e garantire la ripartenza di tutti i servizi, anche su un diverso sito.

Il tempo massimo di ripartenza del Centro Servizi (RTO) è stabilito in 48 ore dall'evento di indisponibilità come indicato nell'Allegato 3 – Indicatori di qualità della fornitura.

La soglia di tolleranza per il ripristino dei dati (RPO) è stabilito in 24 ore secondo quanto stabilito nell'Allegato 4A - Schema di Contratto Quadro .

Il fornitore ha la facoltà di proporre RTO e RPO migliorativi, da inserire come parametri contrattuali; tale proposta sarà valutata secondo quanto riportato nell'apposito criterio nella Lettera d'invito.

I Centri Servizi del Fornitore, dai quali vengono erogati i servizi del presente capitolato, devono essere interconnessi sia alla rete Internet che alla rete SPC. L'interconnessione alla rete Internet deve avvenire per il tramite di almeno due differenti Service Provider.

L'interconnessione alla rete SPC deve avvenire per il tramite di uno dei Fornitori qualificati SPC ai sensi del DLgs 42/2005.
Il dimensionamento delle interconnessioni deve essere effettuato nel rispetto dei Livelli di Servizio che il fornitore deve garantire nei confronti delle Amministrazioni sottoscrittrici dei contratti esecutivi.
Tutte le interconnessioni dei Centri Servizi con la rete SPC e con la rete Internet, per l'erogazione dei servizi contrattualizzati, sono a carico dell' Aggiudicatario.
Per le singole Amministrazioni non è previsto alcun onere aggiuntivo per la predisposizione e l'utilizzo della connessione telematica nell'ambito di ogni servizio.
Il Fornitore deve disporre di un proprio Autonomus System (AS) ed di classi di indirizzi IP ad esso associate. Tali classi dovranno essere annunciate in maniera più specifica verso la rete SPC rispetto alle modalità di annuncio utilizzate verso la rete Internet.
Il fornitore deve farsi carico, qualora richiesto dall'Amministrazione, della pubblicazione dei servizi tramite un Servizio DNS.

4.2. Sicurezza del Centro Servizi

Il Fornitore dovrà garantire, per la propria interconnessione a SPC, la sicurezza delle strutture, dei collegamenti e la riservatezza dei sistemi e delle informazioni attraverso la formalizzazione e l'applicazione di procedure e politiche di sicurezza da adottare al proprio interno. In particolare, è responsabilità del Fornitore assicurare che i Centri Servizi, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni da e verso la rete SPC siano protette mediante l'adozione di adeguati sistemi e metodologie, nel rispetto di quanto stabilito dallo standard ISO/IEC 27001, oltre che gestite in piena conformità con la normativa cogente, come meglio specificato nel §3.3.
Devono comunque essere soddisfatti dal Fornitore, almeno nei punti di contatto tra la rete dei Centri Servizi e la rete SPC, nell'ambito della presente gara, i livelli minimi di sicurezza previsti del sistema SPC, ovvero:

a) devono essere presenti dispositivi di tipo Firewall e sistemi di Network Detection ed Event & Log Monitoring, necessari a rilevare e contenere eventuali incidenti di sicurezza ICT;
b) deve essere istituita una Unità Locale di Sicurezza (ULS) con i compiti di cui all' art. 21, commi 6 e 9 del DPCM 1 Aprile 2008 ove ciascun riferimento al CG-SPC nonche al CERT-SPC deve essere riferito al CERT della PA;
c) devono essere adottate tutte le necessarie misure volte a limitare il rischio di attacchi informatici ed eliminare eventuali vulnerabilità della rete, causate dalla violazione e utilizzo illecito di sistemi o infrastrutture del Fornitore.

In generale, il fornitore deve garantire quanto indicato nel documento "Regole tecniche di sicurezza e funzionamento sistema pubblico Dpcm 1/4/2008".
Nel capitolo, ogni qual volta si indica che il fornitore deve garantire impegni/documenti/informazioni vs AGID, tali impegni potrebbero essere, sulla base delle procedure operative di AGID, rivolti vs il CERT/PA.

Le modalità di attuazione dei suddetti requisiti di sicurezza dovranno essere dettagliate all'interno dei seguenti documenti:

- Documentazione del **Sistema di Gestione della Sicurezza delle Informazioni** (SGSI), consistente in un processo iterativo articolato in successive implementazioni, monitoraggi e successive fasi di riesame e miglioramento (rif. §4.2.1);
- il **Piano della Sicurezza dei Centri Servizi**, che dovrà descrivere approfonditamente le 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 delle Amministrazioni (rif. §4.2.2);
- il **Documento Programmatico della Sicurezza**, che dovrà descrivere le misure, gli strumenti e le risorse che il Fornitore Aggiudicatario metterà in campo al fine di preservare la privacy delle informazioni raccolte (rif. §4.2.3).

Il Fornitore Aggiudicatario dovrà garantire la disponibilità dei documenti sopra elencati nei tempi definiti al par. 7.2.5; tali documenti potranno essere oggetto di osservazioni e richieste di aggiornamento da parte di Consip.
Di seguito si riportano nel dettaglio i requisiti obbligatori per garantire la sicurezza del Centro Servizi.

4.2.1. Sistema di Gestione della Sicurezza delle Informazioni

Il Fornitore dovrà garantire un complesso organizzato di risorse umane e strumentali che risponde ai requisiti di:

- **riservatezza**: le informazioni siano accessibili solo a chi è autorizzato ad averne accesso;
- **integrità**: l'informazione (compreso il sistema operativo) ed i servizi erogati possono essere creati, modificati o cancellati solo dalle persone autorizzate a svolgere tale operazione;
- **disponibilità**: le informazioni ed i servizi che il sistema eroga devono essere fruibili dagli utenti del sistema stesso compatibilmente con i livelli di servizio definiti.

A tale scopo, il Fornitore dovrà prevedere per il Centro Servizi l'instaurazione di un adeguato sistema di gestione della sicurezza delle informazioni (SGSI), consistente in

un processo iterativo articolato in successive implementazioni, monitoraggi e successive fasi di riesame e miglioramento.
Il perimetro di validità del SGSI è quello individuato dai dati gestiti dal Sistema Informativo e dalle risorse e strumenti ad essi afferenti gestiti dal Fornitore relativamente all'erogazione dei servizi contrattuali.

4.2.1.1. Obiettivi di sicurezza

I principali obiettivi che il SGSI del Fornitore dovrà garantire sono:

- assicurare la continuità dei servizi e delle applicazioni;
- minimizzare i danni in caso di incidente e/o di avaria del Sistema Informativo;
- garantire la gestione della sicurezza in linea con la normativa nazionale e con gli standard internazionali;
- normalizzare l'approccio alla gestione della sicurezza, ottimizzando e coordinando le risorse disponibili;
- creare un'organizzazione della sicurezza condivisa, documentata, organica, efficiente e capillare;
- consentire un miglioramento continuo del sistema della sicurezza;
- fornire una metodologia, politiche e procedure per il sistema di gestione;
- garantire gli obiettivi di sicurezza della fornitura da inserire nel Piano di Sicurezza del Centro Servizi (vedi §4.2.2) quali a titolo indicativo:
  - sicurezza logica,
  - sicurezza fisica,
  - sicurezza delle applicazioni,
  - gestione delle utenze (policy per il personale),
  - gestione degli incidenti,
  - continuità operativa.

4.2.1.2. Normativa di riferimento

Il Fornitore dovrà implementare il proprio SGSI in relazione alle specifiche espresse nel presente documento e in considerazione degli standard e della normativa di riferimento, di cui i principali riferimenti sono riportati nel §3.3.

4.2.1.3. Gestione della documentazione del SGSI

Al di là della consegna alla stipula del SGSI (si veda par. 4.2.4), Consip/AgID si riservano la facoltà di richiedere durante la durata del contratto la documentazione di attuazione del SGSI prodotta dal Fornitore, il quale dovrà consegnarla entro 30 giorni

dalla richiesta; tale documentazione dovrà essere mantenuta costantemente aggiornata in relazione alle successive evoluzioni del sistema.

4.2.1.3.1. Procedura di Gestione dei documenti SGSI

La documentazione inerente l'SGSI è uno dei beni del SGSI stesso: va pertanto gestita in modo da assicurarne il livello di protezione adeguato. Per tale documentazione il Fornitore dovrà definire e implementare una procedura che definisca le azioni di gestione necessarie a:

- Riesaminare ed aggiornare i documenti e riapprovare i documenti in caso di modifiche successive;
- Assicurarsi che siano identificati i cambiamenti e l'attuale stato di revisione dei documenti;
- Assicurarsi che le versioni più recenti dei documenti rilevanti siano facilmente identificabili e disponibili prevenendo l'utilizzo non intenzionale di documenti obsoleti;
- Assicurarsi che la distribuzione dei documenti sia controllata.

Il Fornitore dovrà predisporre strumenti e processi di gestione della documentazione opportuni al fine di garantire la conservazione e l'aggiornamento della documentazione di sistema.

4.2.1.3.2. Gestione delle registrazioni

Il Fornitore ha l'obbligo di definire e manutenere le registrazioni che forniscono evidenza della conformità ai requisiti e dell'efficace operatività del SGSI (es.: libro dei visitatori, le registrazioni degli audit e l'autorizzazione per gli accessi fisici e logici, ecc.).

La gestione delle registrazioni attraverso qualsiasi supporto dovrà garantire:

- la leggibilità;
- l'identificazione rapida e puntuale;
- l'archiviazione e protezione adeguata;
- la rintracciabilità e disponibilità secondo necessità.

Ogni persona all'interno del SGSI dovrà essere responsabile per la gestione delle registrazioni di propria competenza. Tutte le registrazioni dovranno essere comunque conservate per un periodo minimo di 5 anni.

Il Fornitore presenterà a Consip/AgID, entro 30 giorni lavorativi dalla richiesta, il documento di Gestione delle Registrazioni, contenente la lista delle registrazioni che saranno gestite, unitamente alle modalità di registrazione delle evidenze.
Il Fornitore dovrà consentire, entro 15 giorni dalla richiesta, a Consip/AgID o al personale da essa designato l'accesso fisico alle registrazioni per tutte le verifiche e gli approfondimenti che si rendessero necessari nel corso della durata del contratto.

4.2.1.4. Gestione degli Audit interni del SGSI

Il Fornitore dovrà condurre audit interni sul suo SGSI ad intervalli pianificati al fine di determinare se gli obiettivi del controllo, i controlli, i processi e le procedure del SGSI:

- sono conformi ai requisiti legali e a quelli definiti nelle politiche della sicurezza e nei regolamenti rilevanti;
- sono efficacemente attuati e mantenuti;
- rispondono ai risultati attesi.

Il Programma degli audit interni definito dal Responsabile della sicurezza del Fornitore dovrà essere predisposto con cadenza almeno annuale e reso disponibile a richiesta di Consip/AGID entro il termine di 30 gioni lavorativi.
Il personale che esegue gli audit dovrà essere stato formato in modo specifico e sottoposto a sessioni periodiche di aggiornamento per assicurare la massima efficacia degli audit.
La programmazione degli audit dovrà assicurare l'indipendenza di giudizio degli auditor impiegati: nessuno potrà valutare le attività nelle quali è direttamente coinvolto a qualsiasi titolo.
Il Fornitore dovrà predisporre entro 30 giorni lavorativi successivi alla data di stipula del Contratto Quadro una procedura documentata di audit interno, da presentare a Consip/AgID su richiesta, nella quale saranno definiti i criteri, ampiezza requisiti e le responsabilità per:

- la pianificazione e la conduzione degli audit;
- il rapporto dei risultati;
- la conservazione delle registrazioni e dei rilievi effettuati;
- la gestione ed eliminazione delle non conformità rilevate;
- la pianificazione, la conduzione e il rapporto delle verifiche sulle azioni correttive intraprese per le non conformità.

4.2.1.5. Gestione delle azioni correttive e preventive del SGSI

A fronte di ogni rilievo (derivante da visite ispettive di Consip/AgID, da audit interni o da segnalazione spontanee) e di ogni incidente il Fornitore dovrà determinare le azioni

da intraprendere per eliminare la causa dei rilievi e degli incidenti allo scopo di prevenirne la reiterazione.

Il Fornitore per ogni rilievo e per ogni incidente dovrà:

- determinare le cause;
- valutare la necessità di intraprendere azioni atte ad assicurare che i rilievi e/o gli incidenti non si ripetano;
- determinare e attuare le azioni correttive necessarie (inclusi la valutazione dei rischi, la formazione del personale, l'aggiornamento dei sistemi, etc.);
- registrare i risultati delle azioni intraprese;
- riesaminare le azioni correttive intraprese.

Ogni incidente e/o rilievo dovrà essere registrato in un apposito Registro delle azioni coerentemente con la procedura documentata di audit descritta nel §4.2.1.4 e reso disponibile a Consip/AgID entro 30 giorni dalla richiesta.

Il Registro dovrà contenere almeno le seguenti informazioni:

- i riferimenti al rilievo/incidente;
- la descrizione delle cause identificate;
- le correzioni e le azioni correttive intraprese;
- le date o il periodo entro il quale dovrà essere verificata, per mezzo di audit, l'efficacia di quanto attuato (follow up);
- le responsabilità per le attività definite;
- i risultati ottenuti;
- la data di riesame da parte di Consip/AgID.

Analogamente si opererà per le azioni preventive, che il Fornitore intraprenderà per prevenire possibili rilievi ed incidenti. Tali azioni, che Consip/Agid si riservano di condividere preventivamente, saranno registrate nel Registro delle azioni.

Il Fornitore dovrà predisporre entro la data di stipula del Contratto Quadro il template contenente i campi del Registro delle azioni, da presentare a Consip/AgID su richiesta.

In ogni caso le azioni preventive saranno precedute/seguite da una puntuale valutazione dei rischi per assicurare l'integrità del SGSI e la completa valutazione di tutti gli aspetti di sicurezza potenzialmente a rischio.

Il Fornitore dovrà predisporre entro 30 giorni lavorativi dalla data di stipula del Contratto Quadro la documentazione descrittiva del processo di Incident Management, contenente i criteri di classificazione degli incidenti di sicurezza cosi come descritto nel successivo §4.2.1.8.1, da presentare a Consip/AgID su richiesta.

4.2.1.6. Riesame del SGSI

Il Fornitore dovrà mantenere con cadenza almeno annuale l'allineamento alle politiche relative al riesame sul SGSI per assicurarsi della sua continua idoneità, adeguatezza ed efficacia, su cui Consip/AGID si riservano di effettuare controlli in un qualsiasi momento.

Il riesame sulle Politiche della Sicurezza delle Informazioni include la valutazione delle opportunità per il miglioramento e la necessità di cambiamenti del SGSI. I risultati del riesame sono chiaramente documentati all'interno di un'apposita Relazione di riesame del Fornitore.

Il Fornitore dovrà predisporre, entro 30 giorni dalla stipula del Contratto Quadro, il template, i contenuti minimi ed il formato con cui inviare la Relazione di riesame, da presentare a Consip/AgID su richiesta.

L'input del riesame dovrà essere costituito da:

- risultati di audit e riesami precedenti del SGSI;
- feedback proveniente dalle parti interessate;
- tecniche, prodotti o procedure, che potrebbero essere utilizzate per migliorare le prestazioni e l'efficacia del SGSI;
- status delle azioni preventive e correttive;
- vulnerabilità o minacce non adeguatamente affrontate nella precedente valutazione del rischio;
- azioni derivanti dai precedenti riesami da parte di Consip/AgID;
- cambiamenti che potrebbero incidere sul SGSI;
- raccomandazioni per il miglioramento indicate da Consip/AgID e/o dal Fornitore stesso.

L'output del riesame dovrà comprendere tutte le decisioni e le azioni che abbiano attinenza con:

- il miglioramento dell'efficacia del SGSI;
- le modifiche da apportare alle procedure che incidono sulla sicurezza delle informazioni, secondo quanto necessario, per rispondere a eventi interni o esterni che possono avere un impatto sul SGSI, compresi i cambiamenti del contesto normativo di riferimento;
- i livelli di rischio e/o i livelli di accettazione del rischio.

4.2.1.7. Valutazione dei rischi

Il Fornitore avrà l'obbligo di realizzare una valutazione dei rischi, con aggiornamento almeno annuale, relativamente alla sicurezza delle informazioni gestite.

Nell'esecuzione della valutazione il Fornitore dovrà tenere conto delle potenziali minacce e delle vulnerabilità dei servizi offerti, al fine di effettuare una valutazione dei rischi sulla quale basare la propria strategia di contenimento degli stessi, fermo restando quanto indicato nei requisiti specificati nel presente capitolato di gara.
Il Fornitore dovrà predisporre, entro 30 giorni lavorativi dalla stipula del Contratto Quadro, un documento contenente la valutazione dei rischi inerenti i Centri Servizi, da presentare a Consip/AgID su richiesta.

4.2.1.8. Incidenti, criticità e malfunzionamenti inerenti la sicurezza

4.2.1.8.1. Rapporti sugli incidenti di sicurezza

Ogni situazione anomala dovrà essere registrata e segnalata alle Amministrazioni interessate dai servizi forniti e, laddove necessario, a Consip/AgID, con gli strumenti definiti nelle apposite procedure di gestione (vedi §.4.2.1.3).
Il personale del Fornitore dovrà essere formato per la pronta reazione agli incidenti e l'attivazione dei canali di risposta.
Il responsabile della sicurezza del Fornitore provvederà ad informare le Amministrazioni coinvolte sui risultati delle attività avviate a seguito della segnalazione.
Il Fornitore, oltre a predisporre strumenti, processi di gestione e documentazione opportuni a supporto dell'implementazione di quanto stabilito nel presente documento, dovrà garantire la registrazione degli incidenti rilevati dal proprio personale o da strumenti di monitoraggio a disposizione dei vari servizi della fornitura. Tali registrazioni confluiranno in un registro unico degli incidenti di sicurezza gestito dal Fornitore e reso disponibile entro 5 giorni dalla richiesta di Consip/AgID.
Il registro degli incidenti viene utilizzato nel corso delle sessioni di aggiornamento della formazione come esempi dell'accaduto, della risposta e delle modalità per evitarli in futuro.
Il registro degli incidenti costituirà anche la base per la raccolta delle evidenze necessarie in caso di procedimenti disciplinari e legali.

4.2.1.8.2. Rapporti sulle criticità di sicurezza

Il Fornitore sarà tenuto ad annotare eventuali minacce o debolezze, osservate o sospettate, da qualsiasi fonte provengano le informazioni al riguardo, sia interna che esterna alle Amministrazioni servite. Le criticità registrate dovranno essere trasmesse tempestivamente alle Amministrazioni per la definizione delle eventuali azioni.
Il Fornitore, oltre a predisporre strumenti, processi di gestione e documentazione opportuni a supporto dell'implementazione di quanto stabilito dall'Amministrazione, dovrà garantire la registrazione (§4.2.1.3.2) delle criticità rilevate. Le criticità

dovranno essere analizzate periodicamente nell'ambito della definizione delle azioni correttive (vedi §4.2.1.5) e preventive. Tali registrazioni confluiranno in un registro unico delle criticità di sicurezza gestito dal Fornitore e messo a disposizione di Consip/AgID su richiesta, nei modi e nei tempi già sopra indicati. Per ulteriori obblighi del Fornitore concernenti le criticità inerenti la sicurezza si faccia riferimento a quanto riportato nel contratto e alle successive indicazioni che Consip/AgID potranno fornire all'Aggiudicatario.

4.2.1.8.3. Rapporti sui malfunzionamenti dei sistemi di sicurezza

I malfunzionamenti dei sistemi di sicurezza (hardware e software) dovranno essere annotati (§4.2.1.3.2) e trasmessi entro 10 giorni dalla richiesta all'Amministrazione. I malfunzionamenti dovranno essere analizzati periodicamente nell'ambito della definizione delle azioni correttive e preventive. Tali registrazioni confluiranno in un registro unico dei malfunzionamenti dei sistemi di sicurezza gestito dal Fornitore e condiviso con l'Amministrazione.
Per ulteriori obblighi del Fornitore concernenti i malfunzionamenti inerenti la sicurezza si faccia riferimento a quanto riportato nel contratto e successive indicazioni che Consip/AgID potranno fornire all'Aggiudicatario.

4.2.1.8.4. Apprendere dagli incidenti, criticità e malfunzionamenti

Incidenti, criticità e malfunzionamenti dovranno essere tempestivamente analizzati dal Responsabile della Sicurezza del Fornitore, il quale provvederà a stilare statistiche in materia di frequenza, tipologia, tempi di fermo/ripristino ecc.
Le analisi dovranno essere utilizzate per:

- la programmazione e conduzione degli audit interni (vedi §4.2.1.4);
- la definizione di eventuali azioni correttive e preventive (vedi §4.2.1.5);
- il riesame delle politiche (vedi §4.2.2.1);
- le sessioni di aggiornamento della formazione (vedi §4.2.2.6).

Il Fornitore produrrà periodicamente (almeno una volta ogni tre mesi) adeguata reportistica, da rendere disponibile a Consip/AgID entro 15 giorni dalla richiesta. Il Fornitore dovrà predisporre entro 30 giorni lavorativi dalla data di stipula del Contratto Quadro il modello di reportistica che intenderà utilizzare nell'analisi degli incidenti, criticità e malfunzionamenti, da presentare a Consip/AgID entro 5 giorni dalla richiesta.

4.2.2. Piano di Sicurezza dei Centri Servizi

Il Piano di Sicurezza dovrà descrivere approfonditamente le modalità logistiche ed organizzative, gli strumenti e 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 dell'Amministrazione.

Consip/AgID si riservano la possibilità di richiedere, nel corso della fornitura, le variazioni ritenute opportune al Piano della Sicurezza dei Centri Servizi predisposto dall'Aggiudicatario.

Nei punti che seguono sono indicati i requisiti che tale Piano deve prevedere, formulati in coerenza con la ISO 27001.

Il Fornitore deve effettuare tutte le attività relative alla sicurezza delle informazioni del SGSI in compliance a tale stardard. Il Fornitore dovrà predisporre strumenti, processi di gestione e documentazione opportuni a supporto dell'implementazione di quanto previsto contrattualmente per tutti i controlli di seguito indicati.

Consip/AgID si riservano la facoltà di richiedere, ogni volta che lo reputino opportuno, una nuova versione o revisione del Piano della Sicurezza del Centro Servizi e della documentazione comprovante la corretta esecuzione delle procedure ed istruzioni previste dal Piano della Sicurezza dei Centri Servizi.

4.2.2.1. Politiche della sicurezza delle informazioni

Quale parte del Piano di Sicurezza il Fornitore dovrà predisporre, nell'ambito dello sviluppo del proprio SGSI per i servizi erogati, un documento che descriva le Politiche di Sicurezza in conformità alle norme applicabili, agli impegni presi in ambito contrattuale e nella propria offerta per la presente gara.

Tale documento dovrà contenere oltre che gli obiettivi ed i principi di base, anche le regole, le procedure operative ed organizzative adottate dal Fornitore per la conduzione dei servizi previsti dal Capitolato.

Il documento, ed ogni suo successivo aggiornamento, sarà consegnato a Consip/AgID su richiesta. La predisposizione e le consegna della prima versione del documento di Politiche di Sicurezza dovrà avvenire alla stipula del Contratto Quadro.

Consip/AgID, in base a quanto stabilito del contratto, disporranno opportune verifiche periodiche sull'implementazione delle Politiche di sicurezza del Fornitore.

4.2.2.2. Organizzazione del Fornitore

Il Fornitore dovrà illustrare nel Piano di Sicurezza la propria organizzazione che sarà chiamata ad interagire con l'Amministrazione.

Il Fornitore nel definire l'affidamento delle responsabilità per la sicurezza delle informazioni all'interno della sua organizzazione dovrà considerare, oltre a quanto previsto dalle norme, quanto specificato nel Contratto Quadro.

4.2.2.3. Sicurezza dell'accesso di terze parti

Il Fornitore dovrà illustrare nel Piano di Sicurezza le modalità con cui garantire la sicurezza delle informazioni da lui gestite e delle strutture di elaborazione delle informazioni oggetto di accessi, elaborate, comunicate a/o gestite da terze parti esterni.

Dovranno essere identificati i rischi per le informazioni dell'Amministrazione e per le strutture di elaborazione delle informazioni, derivanti da processi che coinvolgono parti esterne. Dovranno essere realizzati gli appopriati controlli al perimetro prima di consentire gli accessi. L'accesso al perimetro del Centro Servizi può includere l'accesso:

- fisico, cioè a uffici, stanze con computer, archivi, ecc;
- logico, cioè a ambienti software, database, ecc.

Gli accessi logici sono regolati in base a quanto descritto al §4.2.2.9. Per gli accessi fisici al perimetro (stanze, uffici, archivi, ecc.) dovrà essere prevista l'identificazione del personale secondo quanto descritto al §4.2.2.7. Il personale autorizzato dovrà essere in possesso di opportuni badge di riconoscimento temporaneo o permanente. Il badge temporaneo dovrà essere assegnato previa identificazione della persona e registrazione delle sue generalità e del motivo della visita. I badge dovranno essere esposti e consegnati per verifica al personale in possesso di badge permanenti in caso di richiesta.Tutti gli accessi dovranno essere registrati.

A ciascuno vengono illustrate o consegnate le istruzioni e le prescrizioni relative al tipo di accesso consentito; tali istruzioni dovranno essere accettate esplicitamente (data e firma).

L'accesso a terze parti non dovrà essere consentito finché non siano state espletate le procedure di identificazione e registrazione nelle apposite liste.

Il Fornitore dovrà predisporre strumenti, processi di gestione e documentazione opportuni a supporto dell'implementazione di quanto stabilito, rendendo disponibili tutte le informazioni sugli accessi di terze parti a Consip/AgID entro 15 giorni dalla richiesta.

Le disposizioni relative all'accesso di terze parti si devono basare su un contratto o istruzione operativa formale contenente, o facente riferimento, a tutti i necessari requisiti atti ad assicurare la conformità alle politiche per la sicurezza dell'organizzazione e alle norme vigenti.

Consip/AgID potranno eseguire delle verifiche (audit) sulla gestione dei requisiti di sicurezza nei contratti con terze parti.

4.2.2.4. Gestione degli asset

Il Fornitore dovrà illustrare nel Piano di Sicurezza le modalità con cui conseguire e mantenere attiva un'adeguata protezione degli asset utilizzati per l'erogazione dei servizi forniti.

Gli asset da proteggere nell'ambito del sistema predisposto dal Fornitore sono raggruppabili nelle seguenti categorie:

- hardware;
- software;
- dati;
- documentazioni cartacee;
- supporti di memorizzazione esterni.

Il Fornitore dovrà identificare tutti gli asset dedicati alla fornitura e da gestire, compilando e tenendo aggiornato un inventario di tali asset, da allegare al Piano della Sicurezza. Rientrano negli asset da censire anche le eventuali infrastrutture hardware ad utilizzo non esclusivo dei servizi erogati all'interno della presente fornitura.

4.2.2.5. Classificazione delle informazioni

Il Fornitore relativamente alle sue responsabilità e ai dati dell'Amministrazione che tratterà nell'ambito dei servizi erogati, dovrà formalizzare all'interno del Piano di Sicurezza le linee guida per la classificazione delle informazioni da lui trattate rispetto al loro valore, alle prescrizioni legali, alla sensibilità ed alla criticità. Tali linee guida dovranno contenere i criteri di individuazione delle informazioni che sono da considerarsi sensibili o critiche per le Amministrazioni.

La classificazione dovrà riferirsi sia alle informazioni direttamente trattate dal Fornitore (es. nel corso di attività in cui il Fornitore ha facoltà di trattare dati o informazioni delle Amministrazioni quali i servizi di Open Data, Big Data, realizzazione app e siti web, etc.), sia alle informazioni trattate dal Fornitore in modo indiretto (es. per servizi di tipo IaaS/PaaS/SaaS, sicurezza *as a Service*, …).

4.2.2.6. Sicurezza delle risorse umane

Il Piano della Sicurezza dovrà descrivere le modalità di informazione e formazione del personale coinvolto nell'erogazione dei servizi oggetto della presente fornitura. Tutte le persone fisiche e giuridiche che hanno un ruolo nella gestione della sicurezza delle informazioni (Responsabili e Incaricati al trattamento delle informazioni delle

Amministrazioni e del Fornitore) all'interno della struttura del Fornitore, dovranno essere informate e formate sulle responsabilità associate a detto ruolo, sulle modalità di gestione delle informazioni e sull'utilizzo degli impianti elettronici, dei sistemi informativi, dei servizi cui essi hanno accesso e sulle relative politiche di sicurezza.
Dovranno essere formalizzate le responsabilità delle suddette risorse e la gestione delle stesse deve avvenire secondo un processo definito al fine di garantire:

- la consapevolezza dei soggetti interessati rispetto alle proprie responsabilità legali e per la sicurezza inerenti il trattamento delle informazioni e le conseguenze della mancata conformità ai requisiti legali e per la sicurezza;
- la formalizzazione degli accordi di confidenzialità;
- l'aggiornamento dei profili di responsabilità.

Il Fornitore per tutto il proprio personale che opera nell'ambito dei servizi della presente fornitura dovrà definire un programma di formazione generale al fine di sensibilizzarlo nei confronti della sicurezza. In particolare per il personale con specifiche responsabilità per la sicurezza dovrà definire un programma di formazione specifico sulle politiche e sulle procedure inerenti la sicurezza delle informazioni.
Consip/AgID potranno richiedere di visionare le formalizzazioni degli accordi presi con le risorse in merito al proprio ruolo, nonché i programmi di formazione e il relativo stato di erogazione.

4.2.2.7. Sicurezza fisica e ambientale

Il Fornitore dovrà descrivere nel Piano della Sicurezza le modalità con cui predisporre strumenti, processi di gestione e documentazione opportuni a supporto dell'implementazione per tutti gli ambiti di seguito indicati.

4.2.2.7.1. Aree sicure

Il Fornitore definirà all'interno del Piano di Sicurezza il perimetro di sicurezza fisica di sua competenza. Un perimetro di sicurezza è costituito da una barriera, come un muro, un cancello d'ingresso, un tornello controllato da tessere o una reception.
Il perimetro di sicurezza dovrà essere chiaramente delineato per mezzo di piantine, layout fisici, disegni architetturali e logici dei sistemi ecc. Laddove indispensabile dovranno essere previste le barriere necessarie che ne delimitano l'accessibilità al solo personale autorizzato.
Laddove necessario, le barriere fisiche devono essere estese dal pavimento al soffitto per impedire ingressi non autorizzati o contaminazioni ambientali come quelle causate da incendi e inondazioni.

Le porte di accesso al perimetro, se necessario, devono essere collegate ad un sistema di allarme (incendio, intrusione, allagamento ecc.).

E' responsabilità del Fornitore per le sedi di propria competenza operare e vigilare sul rispetto delle citate regole. Il perimetro così delimitato si definisce anche area protetta o area sicura.

Nella delimitazione delle aree sicure il Fornitore terrà conto:

- della possibilità di danni da incendio, inondazione, esplosioni, tumulti e altre forme di disastro naturale o dovuto all'uomo,
- dei regolamenti e delle norme vigenti in materia di salute e la sicurezza.

Laddove necessario (e possibile) il Fornitore dovrà considerare anche eventuali minacce poste da edifici/terreni confinanti (incendi, allagamenti, smottamenti, atti vandalici ecc.).

Il Fornitore, conformemente alla classificazione delle informazioni (vedi §4.2.2.5) ed al livello di protezione associato alle varie classi di informazione, deve valutare la possibilità di implementare, sotto la propria responsabilità, controlli e linee guida addizionali per lavorare nelle aree sicure. L'integrazione richiesta comprende controlli per il personale, o per terze parti che lavorano nell'area sicura, così come per attività di terze parti che vi hanno luogo.

Si specifica che:

- il personale del Fornitore dovrà essere a conoscenza dell'esistenza di aree sicure e/o delle attività che vi si svolgono solo per quanto necessario;
- il lavoro nelle aree sicure avvenga sempre con supervisione, in modo da prevenire l'opportunità di attività dolose;
- le aree sicure vengano periodicamente controllate;
- al personale di terze parti venga consentito un accesso ristretto alle aree sicure solo quando necessario; l'accesso deve essere comunque registrato e monitorato;
- all'interno dello stesso perimetro possono esistere più aree sicure con differenti criteri di sicurezza. In tal caso vengano chiaramente definite le differenze di gestione;
- in nessun sito incluso nei Centri Servizi (se non esplicitamente autorizzato) sia consentito l'uso di apparecchiature per fotografia, video, audio o altro tipo di registrazione.

4.2.2.7.2. Sicurezza delle apparecchiature

Il Fornitore dovrà prevenire la perdita, il danneggiamento, il furto o la compromissione di asset e l'interruzione delle attività organizzative.

Le attrezzature presenti all'interno del perimetro fisico di competenza del Fornitore devono essere collocate e protette in modo da ridurre i rischi da minacce, pericoli ambientali e opportunità di accessi non autorizzati al fine di:

- minimizzare accessi non necessari alle aree sicure;
- ridurre il rischio di sguardi casuali durante il loro utilizzo.

Il Fornitore dovrà dare evidenza nel Piano della Sicurezza delle misure adottate necessarie per minimizzare i danni derivanti da: furto, incendio, esplosione, fumo, allagamento, ammanchi di erogazione d'acqua, polveri, vibrazioni, effetti chimici, interferenze nell'erogazione di corrente, radiazioni elettromagnetiche anche derivanti da edifici adiacenti.

Il Fornitore deve garantire il monitoraggio delle condizioni ambientali, al fine di evitare condizioni limite che potrebbero incidere sul funzionamento degli impianti di elaborazione delle informazioni. Le registrazioni derivanti dal suddetto monitoraggio saranno gestite conformemente a quanto stabilito nel §4.2.1.3.

Le attrezzature critiche presenti all'interno del perimetro fisico di competenza del Fornitore dovranno essere protette da ammanchi di corrente e da altre anomalie elettriche tramite opportuni sistemi di continuità elettrica. Tutti i siti dove saranno localizzate le attrezzature critiche dovranno essere dotati di sistemi di illuminazione di emergenza in grado di assicurarne l'operatività anche in condizioni critiche.

I cavi per la corrente e per le telecomunicazioni, che trasportano dati o servizi informativi di supporto, dovranno essere protetti da danno.

Lo smaltimento o il riutilizzo negligente delle attrezzature possono compromettere la sicurezza delle informazioni, pertanto si richiede che lo smaltimento o il riutilizzo dei dispositivi contenenti informazioni delicate o critiche avvenga secondo un determinato processo che assicuri la rimozione sicura dei dati. La descrizione di tale processo dovrà essere contenuta nel Piano della Sicurezza.

4.2.2.8. **Procedure operative**

Il Fornitore dovrà definire e descrivere nel Piano di Sicurezza del Centro Servizi le procedure operative e gli strumenti a supporto delle stesse atte a garantire i servizi richiesti. Tali procedure dovranno includere:

- Gestione di servizi di terze parti
- Protezione contro software dannosi e codici autoeseguibili
- Backup e restore
- Gestione della sicurezza di rete
- Trattamento dei supporti rimovibili
- Trasmissione delle informazioni

- Monitoraggio degli accessi e dell'uso dei sistemi

In particolare per quest'ultima fattispecie i controlli selezionati per la attuazione delle politiche di monitoraggio degli accessi e dell'uso del sistema sono di seguito riportati:

- Log di audit – I log di audit che registrano attività degli utenti, condizioni eccezionali ed eventi relativi alla sicurezza delle informazioni, devono essere generati e manutenuti aggiornati per un periodo di tempo prestabiliti;
- monitoraggio dell'utilizzo dei sistemi – Devono essere stabilite procedure per monitorare l'utilizzo delle strutture di elaborazione delle informazioni e i risultati delle attività di monitoraggio devono essere riesaminate regolarmente;
- protezione dei log – Le strutture e le informazioni di logging devono essere protette contro alterazioni e accesso non autorizzato;
- Log degli amministratori e degli operatori – Le attività degli amministratori e degli operatori devono essere registrate cronologicamente (rif. Provvedimento del 27 novembre 2008 -G.U. 300 del 24/12/2008);
- Log degli errori – gli errori devono essere registrati cronologicamente, analizzati e devono essere intraprese le azioni appropriate.

4.2.2.9. **Controllo degli accessi logici**

Il Fornitore dovrà descrivere nel Piano di Sicurezza strumenti, processi di gestione e documentazione opportuni a supporto del controllo degli accessi logici.

Gli accessi ai sistemi informativi dell'Amministrazione sono controllati attraverso processi formali di registrazione e de-registrazione dell'utente che prevedono:

- l'uso di user ID uniche così che gli utenti possano essere collegati alle proprie azioni ed essere resi in tal modo responsabili;
- il controllo che l'utente abbia l'autorizzazione ad accedere al servizio richiesto;
- il controllo che il livello di accesso concesso sia appropriato;
- di mantenere una registrazione formale di tutte le persone che possono usare i vari servizi; la registrazione deve riguardare almeno i seguenti dati della persona: nome e cognome, società di appartenenza, eventuali riferimenti al contratto ed ai servizi, motivazione all'accesso, data di concessione/revoca dell'autorizzazione, frequenza di accesso (occasionale, permanente), livello di autorizzazione concesso, identificativo o userid assegnata,
- di rimuovere immediatamente i diritti d'accesso di utenti per i quali non è più necessario o possibile mantenere tale accesso;
- il controllo periodico di user ID e account ridondanti per rimuoverli;
- di assicurarsi che used ID ridondanti o rimosse non siano concessi ad altri utenti.

4.2.2.10. **Sviluppo e manutenzione dei sistemi informativi**

Con riferimento ai servizi, ove erogati su sistemi presenti sui Centri Servizi, che prevedono la realizzazione di sistemi informativi (presenti nei Lotti 3 e 4) i controlli selezionati per la sicurezza dello sviluppo e manutenzione dei sistemi da includere nel Piano di Sicurezza sono di seguito riportati:

- analisi e descrizione dei requisiti di sicurezza nello sviluppo dei sistemi: i requisiti per lo sviluppo e manutenzione del Sistema Informativo dovranno includere i requisiti per la sicurezza delle informazioni. Il Fornitore ha l'obbligo della gestione della anomalie del software inerenti la sicurezza;
- controlli sulle elaborazioni dei sistemi applicativi. Prevenire errori, perdite, modifiche non autorizzate o utilizzi impropri delle informazioni nelle applicazioni, attraverso:
    - validazione dei dati di ingresso – devono essere validati per assicurare che siano corretti ed appropriati;
    - tenuta sotto controllo dell'elaborazione interna - è necessario individuare alterazioni delle informazioni dovuta a errori di elaborazione o ad azioni deliberate;
    - integrità dei messaggi – devono essere identificati i requisiti per assicurare l'autenticità e proteggere l'integrità dei messaggi all'interno delle applicazioni;
    - validazione dei dati in uscita – devono essere validati per assicurare che l'elaborazione delle informazioni memorizzate sia corretta ed appropriata.
- controlli crittografici: ove necessario, proteggere la riservatezza, l'autenticità e l'integrità delle informazioni a mezzo della crittografia;
- sicurezza dei file di sistema: assicurare la sicurezza dei file di sistema;
- sicurezza nei processi di sviluppo e supporto. Mantenere la sicurezza del software applicativo di sistema e delle informazioni, attraverso:
    - procedura di tenuta sotto controllo dei cambiamenti;
    - riesame tecnico delle applicazioni in seguito a cambiamenti nei sistemi operativi;
    - limitazione ai cambiamenti nei pacchetti software;
    - sviluppo di software affidato all'esterno - tale sviluppo software affidato a terzi, deve essere supervisionato e monitorato dal Fornitore.
- gestione delle vulnerabilità tecniche: ridurre i rischi derivanti dallo sfruttamento di vulnerabilità tecniche pubblicate.

4.2.2.11. Gestione degli incidenti relativi alla sicurezza delle informazioni

Nel Piano di Sicurezza il Fornitore illustrerà le procedure di gestione degli incidenti di sicurezza (vedi anche §4.2.1.8).

4.2.2.12. Gestione della continuità operativa

Il Fornitore dovrà definire e illustrare nel Piano della Sicurezza il processo per lo sviluppo ed il mantenimento della continuità operativa per i processi e sistemi critici evidenziando:

- i rischi in termini di probabilità di verificarsi e di impatto, compresa ove applicabile l'identificazione e l'assegnazione di priorità di intervento;
- l'impatto che le interruzioni potrebbero avere sui servizi erogati;
- la strategia di continuità operativa coerente con gli obiettivi e le priorità evidenziate nella politiche;
- le prove e gli aggiornamenti previsti sui piani e sui processi correlati;
- le responsabilità per la gestione del piano di continuità.

Il processo di gestione della continuità operativa dovrà essere allineato a quanto richiesto dal art. 50bis del Codice dell'Amministrazione Digitale (D.Lgs 235/2010) ed alle linee guida per il disaster recovery delle Pubbliche Amministrazioni redatte da AGID.

Il Piano di continuità dei servizi erogati tramite i Centri Servizi, da includere/allegare al Piano di Sicurezza, dovrà fissare gli obiettivi ed i principi da perseguire, descrivere i ruoli, le responsabilità, i sistemi di escalation e le procedure per la gestione della continuità operativa, tenuto conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche.

I piani per la continuità operativa possono in generale fallire al momento della prova, spesso a causa di presunzioni scorrette, sviste o cambiamenti delle attrezzature o nel personale: essi dovranno pertanto essere provati regolarmente per assicurare che siano aggiornati ed efficaci. Queste prove assicurano che tutto il personale sia a conoscenza dei piani e delle attività in essi contenute.

Le prove devono essere eseguite con cadenza almeno trimestrale e possono includere a titolo esemplificativo e non esaustivo:

- prove a tavolino di vari scenari (discutere le disposizioni per il recupero aziendale usando esempi di interruzioni);
- simulazioni (in particolare per addestrare le persone nei ruoli gestionali post-crisi / incidente);

- prove di recupero tecnico (assicurarsi che i sistemi d'informazione possano essere ripristinati efficacemente);
- prove complete (provare che l'organizzazione, il personale, le attrezzature, gli impianti e i processi possano affrontare le interruzioni);

Il responsabile/referente della sicurezza del Fornitore riesaminerà i piani con frequenza almeno annuale per assicurarne la congruità con gli altri elementi del Piano di Sicurezza, sulla base dei risultati delle prove e delle simulazioni effettuate.

Consip/AgID si riservano la facoltà di accedere (entro 15 giorni dalla richiesta) alla documentazione relativa allo svolgimento delle prove dei piani di continuità operativa, in modo da verificarne la corretta esecuzione da parte del Fornitore.

4.2.3. Documento Programmatico sulla Sicurezza

Il Fornitore aggiudicatario dovrà indicare le procedure e gli strumenti che intende utilizzare per garantire la sicurezza delle informazioni e dei dati trattati e scambiati in termini di Riservatezza, Integrità e Disponibilità.

A tal fine, non solo dovrà garantire e monitorare il rispetto del D.l.vo 196/2003 "Testo unico delle disposizioni in materia di privacy" ma dimostrare che le informazioni siano gestite e conservate sul territorio comunitario.

In particolare, il Fornitore Aggiudicatario dovrà predisporre ed inviare entro 20gg lavorativi dalla richiesta dell'Amministrazione contraente il **Documento Programmatico sulla Sicurezza**, che dovrà riportare:

- la definizione delle linee guida progettuali per la determinazione delle misure di sicurezza minime e idonee per la protezione dei dati informatici e dei relativi flussi;
- il personale coinvolto nel trattamento dei dati quali ad esempio:
  - gli amministratori di sistema,
  - il responsabile del trattamento interno ed esterno,
  - gli Incaricati interni,
  - gli addetti alla gestione e/o alla manutenzione degli strumenti elettronici,
  - i soggetti incaricati della custodia delle credenziali di autenticazione, ecc.) e le relative lettere di nomina.

  Per ciascuno di essi dovranno essere descritti compiti e responsabilità di competenza;
- la Banca Dati (ovvero il data base o l'archivio informatico), con le relative applicazioni, in cui sono contenuti i dati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati. In tal caso le banche dati potranno essere elencate;

- il luogo in cui risiedono fisicamente i dati, ovvero dove si trovano gli elaboratori sui cui dischi sono memorizzati i dati (in quale sede, centrale o periferica, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, ecc.) ed ogni altro supporto rimovibile;
- la tipologia di dispositivi di accesso, cioè l'elenco e la relazione sintetica degli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.;
- la tipologia di interconnessione, cioè la descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, Internet, ecc.;
- i principali eventi potenzialmente dannosi per la sicurezza dei dati (analisi dei rischi), e valutarne le possibili conseguenze e la gravità in relazione al contesto fisico–ambientale di riferimento e agli strumenti elettronici utilizzati (comportamenti anomali da parte degli operatori al servizio, malfunzionamento degli strumenti utilizzati, virus, ecc.);
- i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva dall'eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando sono necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci. Pertanto, è opportuno descrivere sinteticamente anche i criteri e le procedure adottate per il salvataggio dei dati al fine di una corretta esecuzione del loro ripristino;
- il piano degli interventi formativi previsto per gli Incaricati alla responsabilità del trattamento dati e per tutte le risorse identificate come addetti alla sicurezza e alla gestione, soprattutto in relazione di eventi come ingresso in servizio di nuovo personale, cambiamento di mansioni degli Incaricati, introduzione di nuovi elaboratori e/o di programmi e sistemi informatici, ecc.;
- la definizione delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Eventuali variazioni dovranno essere comunicate dal Responsabile dei Centri Servizi tempestivamente.

4.2.4. Consegna di documenti riguardanti la sicurezza del Centro Servizi

Per quanto concerne i documenti:

- Procedura di Gestione dei documenti SGSI,
- Piano della Sicurezza del Centro Servizi,

la mancata consegna ovvero la consegna di documenti aventi contenuti non conformi a quelli minimi indicati darà luogo alla mancata stipula del Contratto Quadro (si veda lettera d'invito – Adempimenti per la stipula del contratto).
Al di là della consegna alla stipula, Consip/AgID si riservano la facoltà di richiedere durante la durata del contratto la documentazione di cui sopra, che dovrà consegnarla entro 30 giorni lavorativi dalla richiesta. Tale documentazione dovrà essere mantenuta costantemente aggiornata in relazione alle successive evoluzioni del sistema.
Consip S.p.A. potrà richiedere al Fornitore, entro 30 (trenta) giorni lavorativi dalla ricezione, le modifiche o integrazioni alla suddetta documentazione che il Fornitore dovrà recepire entro il termine perentorio di 15 (quindici) giorni lavorativi successivi alla comunicazione Consip S.p.A.

In generale, per il resto della documentazione, Consip/AgID si riservano di richiedere la consegna formale dei documenti elencati nel capitolo nei tempi indicati nei singoli paragrafi. La tabella seguente riassume i principali impegni in tal senso assunti dal fornitore nei confronti di Consip/AGID (e della Amministrazioni contraenti per quanto concerne il Documento Programmatico della Sicurezza):

Nome documento	Contenuti previsti	Data di disponibilità
Procedura di Gestione dei documenti SGSI	§4.2.1.3.1	Prima consegna alla stipula del Contratto Quadro; successivi aggiornamenti entro 30gg lavorativi e ad ogni successivo aggiornamento
Gestione delle registrazioni	§4.2.1.3.2	Entro 30gg lavorativi dalla stipula del Contratto Quadro e ad ogni successivo aggiornamento
Programma e procedura Audit	§4.2.1.4	Entro 30gg lavorativi dalla stipula del Contratto Quadro e ad ogni successivo aggiornamento
Template campi del Registro delle azioni	§4.2.1.5	Entro 30gg lavorativi dalla stipula del Contratto Quadro e ad ogni successivo aggiornamento
Processo di Incident Management e criteri di classificazione degli incidenti di sicurezza	§4.2.1.5	Entro 30gg lavorativi dalla stipula del Contratto Quadro e ad ogni successivo aggiornamento
Template per il Riesame del SGSI	§4.2.1.6	Entro 30gg lavorativi dalla stipula del Contratto Quadro e ad ogni successivo aggiornamento
Valutazione dei rischi	§4.2.1.7	Entro 30gg lavorativi dalla stipula del Contratto Quadro e ad ogni successivo aggiornamento
Modulo di reporting per le analisi periodiche di Incidenti, Criticità e Malfunzionamenti	§4.2.1.8	Entro 30gg lavorativi dalla stipula del Contratto Quadro e ad ogni successivo aggiornamento
Report degli Incidenti,	§4.2.1.8	Periodicamente, ovvero almeno una

Nome documento	Contenuti previsti	Data di disponibilità
Criticità e Malfunzionamenti		volta ogni sei mesi
Piano di Sicurezza del Centro Servizi	§4.2.2	Prima consegna alla stipula del Contratto Quadro; successivi aggiornamenti entro 30 gg lavorativi dalla richiesta
Documento Programmatico sulla Sicurezza	§4.2.3	Entro 20gg lavorativi dalla richiesta dell'Amministrazione Contraente

5. Help Desk

Il Fornitore deve garantire e realizzare un servizio di Help Desk, dedicato all'assistenza in remoto, che abbia almeno le caratteristiche descritte di seguito nel capitolo e da considerarsi minime.

5.1. Descrizione

Il servizio di assistenza in remoto è rivolto ai Referenti identificati dalle Amministrazioni e deve fornire un punto di accesso unificato e un insieme di funzioni di assistenza.

Tale assistenza dovrà riguardare:

- **aspetti amministrativi e contrattuali relativi ai Contratti Esecutivi** anche per ciò che riguarda le fasi e attività propedeutiche alla stipula degli stessi; in tal caso, gli utenti target del servizio saranno i Referenti delle Amministrazioni, incaricati della gestione degli aspetti amministrativi in ambito;
- **aspetti funzionali e tecnici dei servizi oggetto della Fornitura**; a tal fine, le Amministrazioni individueranno i propri Referenti funzionali che fungeranno da interlocutori con le strutture dell'Help Desk, gestendo al proprio interno il contatto con gli utenti dei servizi.

Le Amministrazioni contraenti renderanno disponibili al Fornitore le informazioni necessarie (es. lista dei referenti) e, ove disponibile, il numero medio di contatti ipotizzabili nel periodo di riferimento.

Il Fornitore dovrà strutturare il servizio di assistenza in remoto in modo da presentare un'interfaccia unica verso gli utenti ed assicurare la tracciabilità in termini di segnalazioni/azioni intraprese. In particolare deve essere reso disponibile almeno:

- un servizio di help desk telefonico, accessibile attraverso chiamata su un unico numero verde in tempo reale e con un tempo di attesa in coda come da specifico Indicatore di Qualità presente nell'Appendice 1 apposito; un servizio di supporto via e-mail, integrato con il sistema di Trouble Ticketing indicato nel §6.2.3.
- un'interfaccia web che consenta al referente dell'Amministrazione di inoltrare segnalazioni attraverso il sistema di Trouble Ticketing, sopra indicato.

Il servizio di Help Desk deve essere strutturato almeno in due livelli logici:

- Help Desk di primo livello il quale:

- riceve e registra le chiamate dei Referenti, classifica la richiesta e se possibile fornisce direttamente una soluzione, altrimenti smista la richiesta al secondo livello;
- documenta i livelli di servizio dell'intero servizio;

- Help Desk di secondo livello il quale:
  - affronta i problemi non risolti dal primo livello, assegnando una priorità e smistandoli secondo la tipologia;
  - documenta i livelli di servizio del solo secondo livello.

Entro l'orario di lavoro previsto (si veda Capitolo 9), le segnalazioni dovranno essere prese in carico da un addetto con i livelli di servizio definiti per la fornitura e dettagliati nelle relative Appendici ai Capitolati specifici di Lotto. Al di fuori di tale periodo l'Aggiudicatario deve garantire:

- la ricezione delle segnalazioni almeno attraverso il canale "e-mail" e via form web tramite portale;
- la ricezione di segnalazioni relative a malfunzionamenti (dai sistemi interni di monitoraggio) ed alle funzioni di sicurezza in maniera continuativa (24hx7gg);

Nel caso in cui l'Amministrazione disponga già di un Help Desk di primo livello, l'Aggiudicatario ne deve assicurare l'interazione bidirezionale, anche proattiva, con il proprio servizio di Help Desk di secondo livello attraverso opportune procedure di ricezione dei TT e di chiusura degli stessi.

L'Aggiudicatario deve storicizzare le informazioni relative alle segnalazioni pervenute all'Help Desk di primo livello in modo da consentire l'analisi successiva sino al livello del singolo disservizio della singola Amministrazione contraente.

Le informazioni relative alle richieste di assistenza dovranno essere tali da essere riutilizzabili come feed back per la elaborazione di *Frequently Asked Questions* (FAQ), nonché di interventi sull'applicazione e sulla documentazione di corredo.

5.2. Requisiti dell'Help Desk di primo livello

L'Help Desk di primo livello deve provvedere almeno a:

- assicurare la comunicazione tempestiva ed efficace con l'utenza;
- provvedere all'acquisizione e alla registrazione delle richieste di assistenza;
- risolvere le segnalazioni per le quali è nota la procedura di risoluzione;
- smistare al secondo livello la risoluzione dei problemi non risolvibili al primo livello;
- controllare i processi di risoluzione attivati e verificarne gli esiti;
- comunicare all'utente la risoluzione della segnalazione o il suo inoltro al secondo livello;

- produrre statistiche sugli interventi ai fini di successive analisi.

5.3. Requisiti dell'Help Desk di secondo livello

L'Help Desk di secondo livello deve provvedere almeno a:

- fornire assistenza ai referenti delle Amministrazioni per l'uso appropriato dei servizi acquisiti dalle Amministrazioni contraenti;
- fornire assistenza e supporto amministrativo per l'acquisizione dei servizi previsti dalla presente fornitura e la stipula dei Contratti Esecutivi;
- prendere in carico e tracciare le richieste di informazioni e le segnalazioni di guasti e malfunzionamenti, provvedendo alla loro risoluzione;
- notificare il ripristino delle funzionalità all'Help Desk di primo livello;

Costituirà responsabilità dell'Aggiudicatario condurre le previste attività di escalation verso i soggetti terzi (eventualmente indicati dall'Amministrazione) presso cui ha aperto una segnalazione relativa ad un problema ancora insoluto.

5.4. Reportistica di riscontro relativa all'Help Desk

Devono essere previsti dei report di rendicontazione, suddivisi per ogni servizio, rispettivamente a livello giornaliero e mensile e con almeno le informazioni relative a:

- numero di richieste di assistenza ricevute nel periodo;
- distribuzione delle richieste per modalità di accesso al servizio;
- distribuzione delle modalità di intervento (risoluzione immediata, rigetto, smistamento ad altre strutture);
- distribuzione dei malfunzionamenti per severità e priorità di intervento;
- durata media degli interventi;
- durata massima e minima degli interventi;
- livello di servizio rispettivamente raggiunto per l'Help Desk di primo e secondo livello;
- calcolo di eventuali penali.

La reportistica relativa al servizio è archiviata e conservata per tutta la durata contrattuale a cura dell'Aggiudicatario e resa accessibile nelle modalità e con gli strumenti descritti nel successivo § 6.

6. STRUMENTI A SUPPORTO DELL'EROGAZIONE DEI SERVIZI

Nei paragrafi seguenti sono descritti gli strumenti a supporto dell'operatività che dovranno obbligatoriamente essere resi disponibili dal Fornitore per l'erogazione ed il monitoraggio dei servizi per l'intera durata contrattuale.

6.1. Sottoscrizione dei Servizi di Governance

Per garantire la corretta governance dei Servizi alle Amministrazioni aderenti, il Fornitore è obbligato a sottoscrivere con il Gestore delle IC-SPC (Infrastrutture Condivise-SPC), i Servizi di Governance sotto elencati.

L'adesione si renderà effettivamente obbligatoria ed operativa nel momento in cui saranno disponibili le Infrastrutture condivise – SPC a completamento degli esiti della relativa Gara.

Fino all'attivazione dei servizi di governance sulla piattaforma delle Infrastrutture Condivise-SPC, il Fornitore dovra garantire tali servizi alle Amministrazioni e a Consip/Agid attraverso propri strumenti.

I servizi di Governance, erogati tramite una piattaforma informatica facente parte delle Infrastrutture Condivise, che dovranno essere sottoscritti dal Fornitore, sono costituiti da:

- servizio di Gestione Automatizzata dei Contratti (SGAC),
- servizio di Gestione dei Dati di Qualità e Sicurezza (SGQS),
- servizio di Gestione del Portale Web (SGPW).

Il canone dovuto a fronte della sottoscrizione dei servizi di Governance (da considerarsi iva esclusa) è riportato nella seguente tabella:

Listino servizi IC-SPC rivolto ai Fornitori SPC				
Servizi di Governance		Una Tantum	Canone Annuo	Canone Mensile
SGAC	Gestione Automatizzata dei Contratti	11.260,00 €	9.012,00 €	751,00 €
SGQS	Gestione dei Dati di Qualità e Sicurezza	11.260,00 €	9.012,00 €	751,00 €
SGPW	Gestione del Portale Web	5.526,00 €	4.416,00 €	368,00 €

6.1.1. Sottoscrizione del Servizio di Gestione Automatizzata dei Contratti

Il Servizio di Gestione Automatizzata dei Contratti (SGAC) consente la gestione automatizzata dei contratti: conterrà tutti i dati normativi, contrattuali e tecnici di ciascun Contratto Quadro e dei relativi Contratti Esecutivi (inclusi eventuali allegati) stipulati dalle Amministrazioni.

Il servizio permette sia la gestione dei contratti stipulati che di quelli in corso di stipula da parte del Fornitore.

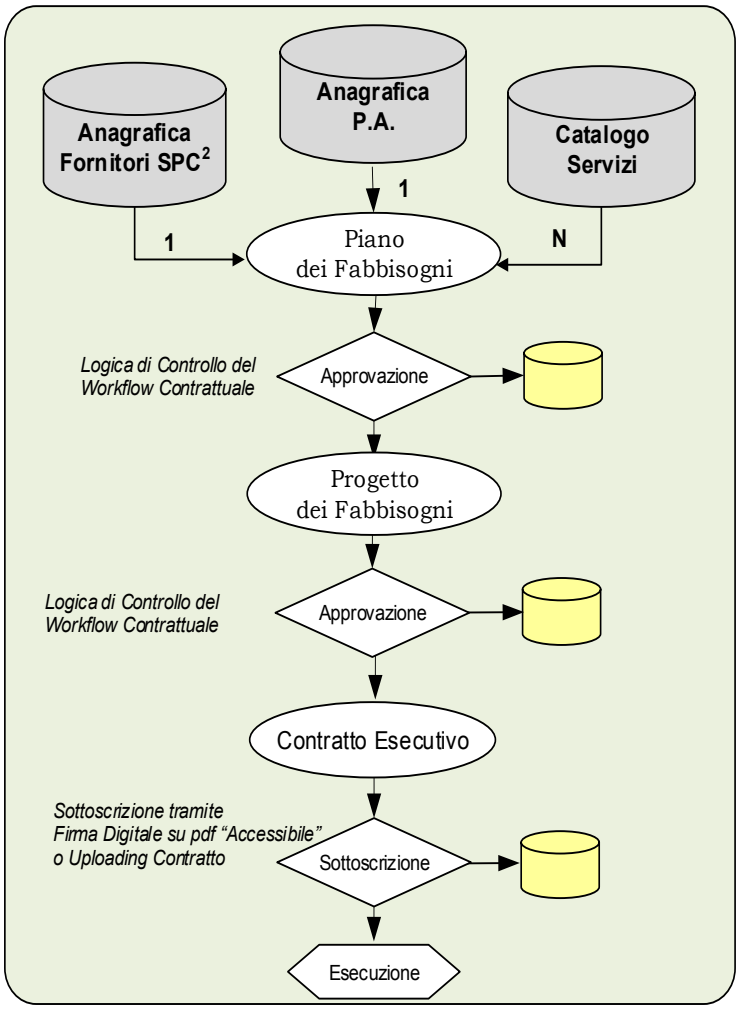
Il Fornitore è obbligato ad aderire al servizio SGAC e a utilizzare il sistema CRUD (*Create, Read, Update e Delete*) messo a disposizione dal Gestore delle IC-SPC come unico strumento per la corretta e formale modellazione dei Piani dei Fabbisogni (da parte delle Amministrazioni) e dei Progetti dei Fabbisogni (da parte dei Fornitori), come riportato nei par. 7.2.3 e par. 7.2.4, attraverso:

- *Web Application*: attraverso il Servizio di Gestione del Portale *Web* di IC-SPC, mette a disposizione le opportune viste e web form;
- *Web Service*: accesso alle funzionalità della piattaforma tramite web service.

Il Servizio di Gestione Automatizzata dei Contratti consente l'interazione, attraverso interfaccia *web*, tra l'Amministrazione che ha aderito o intende aderire ai servizi oggetto di gara e il Fornitore, supportando tutte quelle funzionalità necessarie alla realizzazione e sottoscrizione di un Contratto Esecutivo. In particolare il Fornitore deve:

- caricare sul sistema le informazioni relative alla propria anagrafica e a quella delle Pubbliche Amministrazioni con cui è sottoscritto un Contratto Esecutivo;
- compilare le *webform* relative al *workflow* di gestione "Piano dei Fabbisogni";
- compilare le *webform* relative al *workflow* di gestione dei "Progetto dei Fabbisogni", disponibili al Fornitore solo a valle dell'approvazione da parte dell'Amministrazione sul sistema stesso;
- gestire *on line* il Piano di Attuazione (sottoinsieme del Progetto dei Fabbisogni) e l'eventuale processo di migrazione dei servizi;
- sottoscrivere il Contratto Esecutivo tramite firma digitale o, in alternativa, effettuare l'*upload* del contratto sottoscritto dalle parti;
- gestire, con le opportune azioni correttive, gli allarmi generati su apposita *dashboard* dalla Logica di Controllo del *Workflow* Contrattuale (LWC) e generati dalle inconsistenze sui dati contrattuali inseriti.

La seguente figura schematizza la sequenza logica che regola i legami tra le informazioni contenute nell'anagrafica degli utenti e fornitori, nei Contratti Esecutivi, piani e progetti dei fabbisogni:



6.1.2. Sottoscrizione del Servizio di Gestione dei Dati di Qualità e Sicurezza

Il Fornitore è obbligato ad aderire al Servizio di Gestione dei Dati di Qualità e Sicurezza (SGQS) al fine di garantire all'AgID/Consip il corretto monitoraggio della qualità e della sicurezza.

La piattaforma informatica Dati di Qualità e Sicurezza (DQS) contiene i dati di qualità e sicurezza relativi ai Key Performance Indicators (KPI) di tutti i servizi erogati dal Fornitore e i dati economici relativi ai KPI del Fornitore. Il Fornitore è obbligato ad utilizzare il sistema CMK (Caricamento Massivo dei KPI) per il caricamento massivo dei KPI sul DQS, attraverso:

- una interfaccia *Secure File Transfer Protocol* (SFTP);
- una interfaccia *Web Service*.

Il Fornitore deve gestire, effettuando le opportune azioni correttive, gli allarmi inviati su apposita dashboard dalla Logica di Controllo della Corrispondenza dei KPI (LCCK) e generati dal non corretto caricamento dei dati sul DQS o da non conformità. A titolo esemplificativo si riporta il dettaglio di alcune strutture dati:

- KPI relativi ai singoli servizi: data di inizio e data fine erogazione, quantità di componenti di servizio attive, disponibilità del servizio, Trouble Ticket associati e chiusi (con severità, causa disservizio e tempo di ripristino, ecc.);
- KPI economici relativi al Fornitore: valore complessivo del contrattualizzato, valore complessivo delle penali su ciascun servizio, valore del fatturato annuale di ogni singolo Contratto Esecutivo, ecc.

6.1.3. Sottoscrizione del Servizio di Gestione del Portale Web

Il Fornitore deve aderire al Servizio di Gestione del Portale Web (SGPW).
L'infrastruttura informatica che realizza il Servizio SGPW è costituita da una piattaforma di Content Management System (CMS) in grado di gestire il ciclo di vita dei contenuti.
L'infrastruttura gestisce le seguenti tipologie di utenze:

- non autenticato: utente generico del *World Wide Web* (WWW);
- Fornitore SPC Connettività: utente accreditato rappresentante un Fornitore SPC della presente gara;
- Fornitore Gara Cloud: Fornitore di uno dei Lotti della gara in oggetto;
- gestore PEC: utente accreditato facente parte della struttura organizzativa di un gestore PEC;
- Pubblica Amministrazione: utente accreditato rappresentante una PA che ha aderito (o intende aderire) ai servizi SPC (soggetti di cui all'art. 75, comma 3-bis del d.lgs. 30 dicembre 2010 n.235) o alla gara Cloud;
- soggetto sussidiario con Community Network: utente accreditato facente parte della struttura organizzativa di una Regione o di qualsiasi altro soggetto sussidiario;
- AgID: utente accreditato rappresentante AgID;
- CONSIP: utente accreditato rappresentante Consip
- CERT-SPC: utente accreditato rappresentante la struttura organizzativa dell'AgID che ha la responsabilità del CERT-SPC.

Il portale web è costituito almeno dalle seguenti aree di interesse per il Fornitore:

- "Area informativa": contiene informazioni di carattere generale sul Sistema Pubblico di Connettività e Cooperazione e sulla Gara Cloud (contesto normativo e tecnico, disposizioni della Commissione di Coordinamento, documentazione

tecnico-operativa e contrattuale, ecc.); è visibile a tutte le tipologie di utenza, compresa quella non autenticata.

- "Area Governance dei Servizi per i Fornitori": area accessibile dalle utenze di tipo "Fornitore SPC Connettività" e "Fornitore Gara Cloud" contenente almeno: form per il caricamento dei documenti da pubblicare nell'Area Informativa, form per la compilazione, variazione e la gestione dei Progetti dei Fabbisogni (configurazione di ciascun servizio e dettagli come indirizzo, data di attivazione, ecc.), form per la richiesta di approvazione dei Progetti dei Fabbisogni da parte della Pubblica Amministrazione contraente, informazioni sulle procedure di caricamento dati di qualità e sicurezza.
- "Area Governance dei Servizi per le PA": area accessibile alle utenze di tipo "Pubblica Amministrazione" contenente almeno: form per la compilazione e la variazione dei Piani dei Fabbisogni (solo quantitativa), form per l'approvazione o la richiesta di modifica dei Piani dei Fabbisogni, form per l'approvazione dei Progetti dei Fabbisogni (attraverso l'inserimento della data di firma del contratto); link per l'accesso ad altri servizi delle IC.
- "Area Governance": area accessibile dalle utenze di tipo "AgID" e "Consip" contenente almeno: la form per il caricamento dei documenti da pubblicare dell'Area Informativa; form per l'approvazione o per la richiesta di modifica dei Progetti dei fabbisogni; reportistica personalizzata, cruscotti ed indicatori direzionali basati sui dati presenti nelle varie aree del sistema informativo di Governance; rappresentazione di dati storici e statistici (consistenza e caratteristiche tecniche dei servizi attivati, qualità del servizio, dati economici, ecc.).
- "Area Reportistica dei Servizi": area accessibile dalle utenze di tipo "Fornitore SPC Connettività", "Fornitore Gara Cloud", "Pubblica Amministrazione", "AgID", "Consip" e "CERT-SPC". Contiene almeno le seguenti informazioni: report statici e dinamici relativi ai dati della piattaforma "Anagrafica Unica dei Contratti"; report statici e dinamici relativi ai dati di qualità e sicurezza; reportistica delle penali dovute dai Fornitori SPC e Cloud all'AgID, relative ai contratti quadro ed esecutivi; report statici e dinamici relativi ai valori economici dei contratti esecutivi sottoscritti da ogni singolo Fornitore SPC e Cloud, con evidenza della capacità contrattuale residuale.
- "Area Governance dei Servizi IC-SPC": area accessibile dalle utenze di tipo "Fornitore SPC Connettività", "Fornitore Gara Cloud" e "soggetto sussidiario". Contiene le seguenti informazioni: form per il caricamento dei documenti da pubblicare nell'Area Informativa; catalogo dei Servizi IC-SPC; form per la

gestione automatica dei contratti sottoscritti tra il gestore dei servizi IC-SPC ed i Fornitori Assegnatari; form per la richiesta di intervento a IC-SPC per la risoluzione di escalation tecniche e di sicurezza attraverso il Servizio di Gestione delle Escalation.

- "Area Reportistica dei Servizi IC-SPC": area accessibile dalle utenze "Fornitore SPC Connettività", "Fornitore Gara Cloud", "soggetto sussidiario", "AgID" e "CERT-SPC". Contiene report statici e dinamici su consistenza, utilizzo, qualità, sicurezza dei servizi IC-SPC erogati dal Prestatore delle IC-SPC ai Fornitori Assegnatari.
- "Area Governance CERT-SPC": area accessibile unicamente al profilo "Cert-SPC".

6.2. Sistemi di governo e gestione della fornitura

Nei paragrafi seguenti sono descritti gli strumenti a supporto del governo e della gestione della fornitura che dovranno obbligatoriamente essere resi disponibili dal Fornitore per l'intera durata contrattuale.

6.2.1. Portale di Governo e Gestione della Fornitura

In relazione agli ulteriori dati necessari al governo della fornitura, Il Fornitore di ciascun Lotto dovrà rendere disponibile un "Portale di Governo e Gestione della Fornitura" accessibile in modalità web, a ciascun utente abilitato (di Amministrazioni, altri Fornitori abilitati, di Consip/AgID) mediante login e password assegnate. Tale portale dovrà almeno:

- rendere disponibile un cruscotto sintetico di controllo/monitoraggio tecnico/operativo della fornitura, sulla base dei dati di propria competenza;
- rendere accessibili tutte le funzionalità e la reportistica relativa al monitoraggio tecnico/operativo della fornitura;
- rendere accessibili tutte le funzionalità e la reportistica forniti dal "Sistema di Trouble Ticketing – TT" di cui al successivo §6.2.3;
- rendere accessibili tutte le funzionalità e la reportistica forniti dal "Sistema di Gestione Documentale - SGDOC" di cui al successivo §6.2.3;
- mettere a disposizione di ciascun utente abilitato i soli dati di propria competenza;
- rendere disponibili funzionalità di gestione e profilazione utenti.

Il portale dovrà essere reso disponibile a far data dall'attivazione dei servizi del primo Contratto Esecutivo di fornitura sottoscritto e dovrà essere reso disponibile con

continuità alle Amministrazioni contraenti, a Consip, ad AgID e ad eventuali strutture da essi delegate per tutta la durata contrattuale ed aggiornato con frequenza almeno mensile, entro il 15 del mese successivo al mese di riferimento.

Il portale deve essere gestito globalmente dal Fornitore che assume la responsabilità di garantire:

- l'hosting della piattaforma;
- la gestione e manutenzione del portale;
- l'aggiornamento dei contenuti e la corretta alimentazione del sito;
- la disponibilità in linea per le Amministrazioni, Consip/AgID;
- la gestione degli accessi agli utenti abilitati mediante credenziali di riconoscimento (es., login e password);
- la disponibilità di un manuale di utilizzo del portale e dei singoli sistemi integrati;
- la disponibilità di un servizio di supporto tecnico e funzionale agli utenti, secondo quanto definito per l'intera fornitura (cfr. capitolo 5).

Tutta la reportistica prodotta relativa ai servizi dovrà essere archiviata e conservata a cura del Fornitore, attraverso un sistema di gestione della documentazione riservata.

6.2.2. Cruscotto sintetico di controllo/monitoraggio della fornitura

Su richiesta dell'Amministrazione, il Fornitore dovrà rendere disponibile all'Amministrazione stessa, ad eventuali altri Fornitori abilitati, a Consip/AgID, un cruscotto con accesso via web con una vista sintetica degli indicatori relativi alle prestazioni generali dei singoli servizi acquistati e sull'avanzamento in termini di valore economico consuntivato rispetto al valore della singola fornitura e del Contratto Esecutivo. Il cruscotto dovrà essere funzionante entro 30 giorni dalla richiesta.

Per i servizi che lo prevedono, il Fornitore dovrà installare, previa accordo con l'Amministrazione contraente, sonde e/o strumenti per la raccolta dati presso le Amministrazioni.

6.2.3. Sistema di Trouble Ticketing

Il Fornitore di ciascun Lotto deve realizzare e/o mettere a disposizione obbligatoriamente un "Sistema di Trouble Ticketing - TT" per:

a. la gestione dei TT aperti proattivamente dal Fornitore stesso;
b. la gestione dei TT aperti da CONSIP/AgID e dalle Amministrazioni contraenti;
c. l'assegnazione di TT al secondo livello;
d. la riassegnazione di TT aperti in situazioni nelle quali l'ambito di competenza non sia individuato;
e. il monitoraggio dello stato di avanzamento dei TT aperti.

La registrazione delle segnalazioni di malfunzionamento e delle richieste di servizio deve avvenire attraverso l'utilizzo del sistema di TT che dovrà tracciare almeno le informazioni minime seguenti:

- codice identificativo del TT;
- descrizione della segnalazione (malfunzionamento, richiesta di servizio);
- modalità di ricezione (telefono, internet, etc.);
- data ed orario di apertura;
- soggetto che ha richiesto l'intervento;
- elenco e numero di elementi complessivamente coinvolti dal malfunzionamento;
- classificazione della segnalazione (priorità, severità, etc);
- riferimenti operativi coinvolti nel caso specifico;
- smistamento al secondo livello qualora non fosse possibile fornire la soluzione;
- stato del TT;
- descrizione della soluzione;
- diagnosi del malfunzionamento, ove applicabile;
- -data ed orario di chiusura.

6.3. Sistema di gestione documentale

Su richiesta di Consip, Il Fornitore di ciascun Lotto dovrà rendere disponibile all'Amministrazione, ad altri Fornitori abilitati, a Consip/AgID, un sistema di gestione documentale, per archiviare, classificare ed organizzare la documentazione amministrativa ed operativa della singola fornitura e del Contratto Esecutivo.
Il sistema dovrà essere implementato utilizzando un'infrastruttura hardware e software che il Fornitore stesso provvederà a realizzare e mantenere in esercizio. Il Fornitore procederà alla realizzazione del sistema sulla base di quanto proposto nell'Offerta Tecnica.

6.4. Informativa periodica sulla evoluzione tecnologica dei servizi

Il Fornitore dovrà obbligatoriamente supportare Consip e AgID nell'effettuare periodicamente una attività di informazione e condivisione nei confronti delle Amministrazioni e di altri soggetti da queste individuati in merito a tematiche e problematiche inerenti:

- l'evoluzione tecnologica relativa ai servizi oggetto del presente Capitolato ed a nuovi servizi analoghi potenzialmente integrabili a catalogo sulla base delle valutazioni del Comitato;
- l'evoluzione relativa alle modalità di erogazione di servizi ICT che si affermano sul mercato;
- l'evoluzione nelle modalità di tariffazione e pagamento dei servizi;
- le potenzialità offerte alla Pubblica Amministrazione dalle innovazioni di cui ai punti precedenti.

L'informativa sarà effettuata con cadenza almeno annuale, per un numero massimo di tre sessioni, con 50 partecipanti ciascuna.

L'attività dovrà avere inizio sei mesi dopo la data di adesione della prima Amministrazione ai servizi del presente Capitolato.

Il Fornitore renderà disponibile adeguati locali con le eventuali dotazioni tecnologiche finalizzate allo svolgimento della informativa e relativo materiale cartaceo e digitale a supporto e, laddove opportuno, potrà proporre anche soluzioni tecnologiche alternative alla formazione in aula (es. *elearning*).

Il Fornitore dovrà altresì essere disponibile ad attrezzare ed erogare le sessioni informative/formative presso locali indicati da Consip/AgID.

L'agenda dei contenuti proposti per la singola sessione dovranno essere pubblicati, almeno annualmente, sul portale di governo e controllo della fornitura, in modo da consentire agli utenti delle Amministrazioni l'iscrizione alle sessioni dell'informativa.

Il sito di cui sopra renderà disponibile, per ciascuna informativa, un numero di iscrizioni per ogni Amministrazione che sia compatibile con il numero massimo di partecipanti stabilito sopra.

Il Fornitore renderà disponibile il materiale cartaceo e digitale a supporto dell'Informativa periodica.

6.5. Piano della qualità Generale

Al fine di assicurare che la fornitura rispetti i requisiti di qualità il Fornitore di ciascun Lotto dovrà obbligatoriamente predisporre entro 30 giorni lavorativi dalla stipula del Contratto Quadro un Piano della Qualità Generale. Il Piano della Qualità Generale definisce le caratteristiche qualitative cui deve sottostare l'intera fornitura relativamente alla erogazione dei singoli servizi ed a quanto previsto per l'erogazione degli stessi tramite il Centro Servizi nel presente capitolo 4. Il Piano della Qualità Generale dovrà essere redatto dal Fornitore sulla base del manuale di qualità e secondo l'Indice del Piano della qualità contenuto nella Deliberazione 49/2000, 9 novembre

2000, - “Regole tecniche e criteri operativi per l’utilizzo della certificazione EN ISO 9000 nell’appalto di contratti relativi a progettazione, realizzazione, manutenzione, gestione e conduzione operativa dei sistemi informativi automatizzati (Pubblicata nella G.U. 20 dicembre 2000, n. 296, S.O.).

Consip/AgID si riservano la facoltà di verificare il Piano della Qualità Generale predisposto dal Fornitore e di richiederne, laddove ritenuto necessario, l’integrazione o modifica.

7. MODALITÀ DI ESECUZIONE FORNITURA

7.1. Premessa

In questo capitolo si descrivono le modalità di esecuzione della fornitura previste per i servizi oggetto della fornitura; al Comitato è data facoltà di modificare le modalità di esecuzione descritte, di introdurre nuove modalità, di definire/modificare gli attuali standard, anche in corso d'opera.

Per tutti i servizi erogati nell'ambito del presente Contratto Quadro, i Fornitori Aggiudicatari dovranno obbligatoriamente garantire:

- rispetto dei processi, degli standard e di eventuali linee guida adottate dalle Amministrazioni contraenti;
- produzione e disponibilità, almeno in lingua italiana, di tutta la documentazione a seguito delle attività oggetto dei servizi.

7.2. Modalità di esecuzione

Si riportano di seguito le modalità di esecuzione previste per la presente fornitura e si rimanda ai Capitolati Speciali per i dettagli relativi ai singoli servizi previsti.

7.2.1. Modalità 1 – Progettuale

I servizi oggetto della fornitura da erogare in modalità progettuale dovranno essere scomposti in obiettivi e/o interventi e per ognuno di essi il Fornitore Aggiudicatario dovrà redigere un piano di lavoro, indicante le fasi – convenute con l'Amministrazione committente – le relative milestones e i deliverable stabiliti; in particolare, tale pianificazione dovrà prevedere stime caratterizzate da adeguati livelli di precisione/dettaglio e dovrà pianificare almeno i seguenti eventi:

- **richiesta stima**, effettuata dall'Amministrazione al Fornitore, finalizzata alla valutazione dei tempi e dei costi dell'obiettivo e/o intervento, all'interno dei vincoli indicati dall'Amministrazione stessa;
- **comunicazione della stima** dei tempi e dei costi dell'obiettivo e/o intervento, effettuata dal Fornitore;
- **autorizzazione**, con la quale l'Amministrazione contraente autorizza, mediante comunicazione formale;
- **avvio attività,** mediante riunione di kick off con cui l'Amministrazione autorizza , l'avvio formale delle attività relative all'obiettivo e/o intervento stimato;
- **consegna**, che rappresenta la milestone con cui il Fornitore rilascia i prodotti realizzati e, contestualmente, l'Amministrazione ne verifica la quantità e la tipologia senza alcuna valutazione di contenuto;

- **collaudo e verifica di conformità**, effettuati dall'Amministrazione e corrispondenti alla valutazione con verifica di merito dei prodotti consegnati. Realizzata con esito positivo determina, per prodotti intermedi, l'approvazione, per prodotti finali l'accettazione dell'obiettivo e/o output dell'intervento. In caso di sviluppo software tale verifica corrisponde al collaudo del software prima del suo rilascio in esercizio.

Le fasi, i prodotti delle attività e i criteri di fine fase saranno concordati in funzione delle caratteristiche specifiche dei servizi erogati ed il piano di lavoro sottoposto all'approvazione dell'Amministrazione contraente.

La richiesta di stima di un obiettivo e/o di un intervento sarà effettuata dall'Amministrazione comunicando al Fornitore le informazioni necessarie, quali ad esempio:

- data prevista di inizio attività;
- data prevista di fine attività;
- eventuali date/scadenze critiche e/o vincolanti per il Fornitore;
- eventuale tetto/massimale di spesa;
- riferimenti a documentazione esistente (ad esempio studi di fattibilità, requisiti utente già espressi, ecc.

Il dimensionamento degli obiettivi in termini di impegno progettuale dovrà essere espresso secondo la metrica di dimensionamento prevista per lo specifico servizio.
Per gli obiettivi misurati in Punti Funzione le misure, stimate o effettive, dovranno essere rilevate nei seguenti momenti specifici dell'attività progettuale:

- **definizione dei requisiti**, in corrispondenza della quale è richiesta la stima iniziale;
- **analisi** (o fase equivalente), durante la quale è possibile la revisione in funzione di scostamenti nei requisiti utente iniziali. L'Amministrazione può fissare uno scostamento massimo accettabile e dovrà, in ogni caso, approvare la nuova stima;
- **fine realizzazione**, alla quale corrisponde la produzione del consuntivo dell'obiettivo.

Resta inteso che nel caso in cui i conteggi successivi alla stima iniziale risultino inferiori alla stima/misurazione precedente, tale dimensione aggiornata sostituisce la stima iniziale ai fini della fatturazione.
Si precisa inoltre che l'Amministrazione contraente si riserva la possibilità di richiedere una stima aggiornata dei Punti Funzione in ogni momento durante tutto il ciclo di vita dell'obiettivo, anche durante il collaudo.

Il dimensionamento in Punti Funzione degli obiettivi dovrà essere effettuato secondo le modalità di conteggio IFPUG 4.3 o successive e nel rispetto di eventuali standard integrativi in uso presso l'Amministrazione committente.
Per ulteriori dettagli si rimanda ai capitolati tecnici speciali di Lotto.

7.2.2. Modalità 2 – Continuativa

I servizi da erogare in modalità continuativa non sono scomponibili in fasi e richiedono un presidio continuo sulle attività previste; l'attivazione dei servizi in modalità continuativa può avvenire nel rispetto delle date previste nel Progetto dei Fabbisogni. In particolare, i servizi a canone definiti sulla base di "fasce incrementali" (es., fascia 1: utenti da 1 a 250; fascia 2: utenti da 251 a 500 ecc..) sono remunerati attraverso la distribuzione delle quantità per le singole fasce. Rimanendo all'esempio in oggetto, nel caso di un ordinativo di 400 utenti, i primi 250 vengono valorizzati al prezzo della fascia 1, gli altri al prezzo della fascia 2.

I servizi in oggetto devono essere definiti nel Progetto dei Fabbisogni, come di seguito descritto. La regolamentazione contrattuale di tali servizi, la pianificazione e il riepilogo delle risorse impegnate, può essere in giorni/persona, con modalità a tempo e spesa oppure a canone, come dettagliato nella documentazione dei singoli lotti per ogni servizio.
In ogni caso, le attività pianificabili dovranno essere stimate a preventivo, sia in termini di impegno che di date di completamento e le eventuali variazioni dovranno essere comunicate con congruo preavviso e concordate con l'Amministrazione.

7.2.3. Piano dei fabbisogni

Il Fornitore deve impegnarsi obbligatoramente a supportare l'Amministrazione nella redazione di un documento intitolato Piano dei Fabbisogni, contenente per ciascuna categoria di servizi, indicazioni di tipo quantitativo di ciascun servizio che la stessa intende sottoscrivere.

La redazione del "Piano dei fabbisogni" dovrà avvenire, attraverso la compilazione delle *webform* relative al *workflow* di gestione dei "Piani dei Fabbisogni" messo a disposizione dai Servizi di Governance (cfr. cap.6).

Nelle more della realizzazione dei servizi di Governance, la consegna delle informazioni richieste al requisito precedente sarà realizzata tramite l'invio, mediante Posta Elettronica Certificata (PEC) ad una casella di PEC specifica del Fornitore. In questo

caso sarà cura dell'Amministrazione con l'ausilio del Fornitore riportare le informazioni corrette all'interno dei *webform* sopra citati appena questi ultimi si rendano disponibili.

Il Piano dei Fabbisognidovrà essere sempre mantenuto allineato con quanto richiesto dalle Amministrazioni.

Con specifico riferimento ai servizi da svolgere presso i siti delle Amministrazioni, il Fornitore ha facoltà di condurre, con proprio personale tecnico o altro personale da lui stesso incaricato, e congiuntamente con i referenti dell'Amministrazione interessata, sopralluoghi sui siti, allo scopo di verificare gli impatti e le modalità dell'attivazione dei servizi nella sede in esame (secondo quanto richiesto dall'Amministrazione nel Piano dei Fabbisogni).
Il Fornitore deve approntare, ove necessario ed entro 15 gg lavorativi dalla richiesta (o salvo diverso accordo tra le parti), il calendario dei sopralluoghi necessari, che deve indicare, per ciascuna sede oggetto di sopralluogo, il nominativo dell'incaricato dal Fornitore che effettuerà il sopralluogo, con gli estremi di un documento di riconoscimento e l'elenco delle verifiche da effettuare. Il calendario viene sottoposto all'approvazione dell'Amministrazione interessata.

7.2.4. Progetto dei Fabbisogni

Il Fornitore deve obbligatoriamente predisporre entro il termine di 45 giorni solari dal ricevimento del "Piano dei Fabbisogni" un documento intitolato "Progetto dei Fabbisogni", nel quale raccogliere e dettagliare le richieste dell'Amministrazione, contenute nel Piano dei Fabbisogni, e formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nel Contratto Quadro.

Il "Progetto dei fabbisogni" deve contenere i seguenti allegati:

a) "Progetto di Attuazione": con il dettaglio, per ciascun servizio, di:
   - identificativo del servizio;
   - configurazione (ove applicabile);
   - quantità;
   - costi;
   - indirizzo o indirizzi di dispiegamento (nel caso di servizi centralizzati si può riportare anche il solo indirizzo della sede centrale);
   - data prevista di attivazione;

- impegno delle eventuali risorse professionali previste;
- descrizione per lo specifico servizio della struttura funzionale ed organizzativa del centro servizi, completa dei nomi e dei ruoli delle figure responsabili per ciascuno dei servizi, nonché delle relative procedure di escalation;
- specifiche di collaudo, contenenti le modalità di esecuzione dei test di collaudo, descritti tramite schede tecniche di dettaglio e le date di prevista disponibilità al collaudo;

b) "Modalità di presentazione e approvazione degli Stati di Avanzamento mensili"; su richiesta dell'Amministrazione, il Fornitore deve sottoporre all'Amministrazione medesima, con cadenza mensile a partire dalla data di approvazione del Progetto stesso ed entro il giorno 15 del mese successivo al mese di riferimento, uno "stato di avanzamento" redatto come segue, soggetto ad approvazione da parte dell'Amministrazione Beneficiaria.

   Lo "stato di avanzamento" deve contenere almeno le seguenti informazioni e quant'altro ritenuto opportuno dal Fornitore:

   - esito dei collaudi effettuati e collaudi previsti nel mese successivo;
   - varianti e modifiche emerse nel periodo;
   - ritardi verificatisi nelle attivazioni rispetto alle date previste nel Piano di Attuazione del Progetto dei Fabbisogni;
   - malfunzionamenti verificatisi nel periodo.

c) "Piano di Attuazione", articolato nei seguenti allegati:
   - "Piano di lavoro", contenente l'elenco delle attività/fasi previste con le relative date di inizio e fine,
   - "Documento programmatico di gestione della sicurezza dell'Amministrazione";
   - "Piano della qualità" dello specifico servizio contenente la descrizione dettagliata degli obiettivi di qualità relativi al servizio erogato e la descrizione sintetica dei processi di controllo della qualità.

L'Amministrazione ha la facoltà di approvare il "Progetto dei Fabbisogni", ovvero di comunicare la richiesta di eventuali modifiche. In tal caso l'Aggiudicatario dovrà apportare al documento presentato le eventuali modifiche/integrazioni richieste. L'Aggiudicatario dovrà inviare la versione definitiva entro 15 giorni solari dalla comunicazione di richiesta dell'Amministrazione contraente. L'Amministrazione può

richiedere aggiornamenti del Progetto dei Fabbisogni ogni qualvolta lo ritenga necessario.

In particolare, il "Piano di Attuazione" deve includere la descrizione dettagliata delle attività e procedure che il Fornitore metterà in atto nel processo di subentro dei servizi, nei casi in cui tale attività sia richiesta, al fine di minimizzare l'impatto sull'operatività dei servizi erogati. Inoltre, tutte la fasi previste dal piano devono indicare con chiarezza gli obiettivi, i tempi necessari comprensivi delle date da garantire, i deliverables prodotti e le date di consegna.

L'Amministrazione approva il Progetto dei Fabbisogni mediante la stipula del Contratto Esecutivo. Il progetto dei Fabbisogni potra essere aggiornato dall'Amministrazione nel corso del tempo in termini di tipologia di servizi e quantità.

7.2.5. Vincoli temporali sulle consegne

L'Amministrazione sottopone ad Accettazione/Approvazione tutti i prodotti previsti per i servizi attivati nei relativi Contratti Esecutivi, al fine di verificare, a valle della consegna da parte del Fornitore, la rispondenza dei prodotti stessi ai requisiti stabiliti (funzionali e non funzionali).
Di seguito sono riportati i termini entro cui devono essere consegnati i prodotti, salvo diversi accordi con l'Amministrazione, fermo restando che tutte le date di consegna dovranno essere riportate nel Piano di lavoro e che il dettaglio, o ulteriori nuove scadenze potranno essere indicati nell'ambito del singolo progetto/attività.
I prodotti modificati su richiesta dell'Amministrazione contraente dovranno essere riconsegnati corretti entro 5 gg lavorativi dalla formalizzazione, da parte dell'Amministrazione, della richiesta di integrazione/modifica, fatta eccezione per il Piano della qualità generale, per il quale il termine di riconsegna è fissato a 10 gg lavorativi dalla suddetta formalizzazione.
Eventuali ritardi nella risoluzione delle anomalie riscontrate comporteranno l'applicazione delle sanzioni contrattualmente previste.
Elenco dei vincoli:

- Dalla stipula del Contratto Esecutivo

  Il Piano di Subentro (phase-in) ad inizio fornitura (si veda 7.3), quando applicabile, dovrà essere consegnato dal Fornitore di ciascun Lotto entro 20 gg lavorativi dalla data di stipula del Contratto Esecutivo; sulla base di quanto definito nel Piano di Subentro, dovranno essere consegnati anche gli ulteriori documenti previsti, compresi gli inventari degli oggetti sw/hw laddove previsti;
- Nel corso della fornitura

Per tutti i documenti riguardanti le attività progettuali o continuative, la scadenza di consegna è fissata in 5 gg lavorativi dalla richiesta, salvo diversa richiesta dell'Amministrazione contraente.

Per i documenti relativi ad attività propedeutiche all'erogazione dei servizi, la consegna deve avvenire entro 10 gg lavorativi dalla richiesta dell'Amministrazione contraente.

- Al termine della fornitura

  Entro 20 gg lavorativi dalla richiesta dell'Amministrazione contraente, congiuntamente al Fornitore entrante (laddove previsto), il Fornitore dovrà redigere e consegnare il Piano di *phase out*.

- Dalla richiesta dell'Amministrazione

  Per i documenti di seguito riportati, il Fornitore Aggiudicatario dovrà garantire disponibilità entro 20 gg lavorativi dalla richiesta:

  - Documentazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI),
  - Piano della Sicurezza dei Centri Servizi,
  - Documento Programmatico della Sicurezza.

All'atto dell'accettazione dei prodotti, in caso in cui sia possibile procedere all'accettazione/approvazione dei prodotti, verrà redatto e sottoscritto dall'Amministrazione il verbale di accettazione.

7.2.6. Consolidamento delle modalità di esecuzione della fornitura

Propedeutica alla messa a punto dei servizi, e ove ritenuto necessario anche ai collaudi descritti nei successivi paragrafi, è prevista una fase di consolidamento delle modalità di esecuzione dei servizi oggetto della presente gara, nella quale il Fornitore dovrà illustrare a Consip/Agid in un ulteriore dettaglio rispetto a quanto espresso in offerta tecnica le modalità operative attuative di quanto presentato nell'offerta stessa. Consip/Agid si riservano di chiedere al Fornitore integrazioni alle modalità proposte anche in una fase successiva all'attivazione dei servizi.

7.2.7. Collaudi

Si descrivono di seguito le procedure di collaudo che il Fornitore dovrà obbligatoriamente attuare ai fini della verifica della completa funzionalità dei servizi erogati e dei Centri Servizi utilizzati.

In particolare, la fornitura dei servizi descritti nel presente capitolato tecnico potrà essere soggetta alle seguenti procedure di collaudo:

- *collaudo funzionale* (*Test Bed*), svolto da Consip/AgID, che potranno richiedere delle prove mirate a verificare le modalità con le quali il Fornitore erogherà i servizi oggetto della presente gara. Tale richiesta è inerente i servizi elencati nel § 7.2.6.1, ferma restando la facoltà di Consip/Agid di integrare tale elenco;
- *collaudo di servizio*, svolto dalla singola Amministrazione contraente e volto a verificare la corretta erogazione dei servizi/prodotti acquisiti dall'Amministrazione.

7.2.7.1. Collaudo funzionale (*TEST BED*)

Il Fornitore dovrà obbligatoriamente mettere a disposizione di Consip/AgID una piattaforma tecnica (Test Bed), per tutta la durata del Contratto Quadro, che consenta l'esecuzione di prove di collaudo atte a verificare la conformità dei servizi erogati a quanto richiesto dal Capitolato Tecnico e ad eventuali modifiche concordate in corso d'opera dal Comitato di Direzione Tecnica.
Di seguito i requisiti minimi richiesti.
Il Fornitore dovrà realizzare la piattaforma di *Test Bed* presso sedi individuate congiuntamente con CONSIP/Agid, ovvero presso uno dei Centri Servizi utilizzati per l'esercizio, strutturandola in modo tale da consentire l'esecuzione delle verifiche funzionali per i servizi richiesti. Nell'ambito della predisposizione del Test Bed, il Fornitore dovrà fornire anche il personale necessario all'esecuzione delle prove.

In particolare, la piattaforma dovrà, lotto per lotto, garantire almeno il test dei seguenti servizi:
Lotto 1: Servizi Iaas/Paas/Saas;
Lotto 2: l'infrastruttura di gestione delle identità i servizi di firma digitale remota, di timbro elettronico e dei di sicurezza erogati in modalità as a services.
Lotto 3: l'infrastruttura di gestione delle porte di dominio.

Inoltre, per tutti i 4 lotti, il test bed dovrà garantire verifiche su:

- il portale di governo e gestione della fornitura,
- i pannelli/console di acquisto/configurazione dei servizi (laddove previsto, es. Lotto 1),
- gli strumenti di monitoraggio dei servizi, compresa l'interazione con i servizi di governance.

Nel collaudo, Consip/Agid si riservano di verificare la rispondenza dei Centri Servizi ai requisiti minimi (e migliorativi, ove offerti), con una particolare attenzione a quanto concerne le policy di sicurezza adottate.

Ai fini dell'esecuzione delle prove di Collaudo, il Fornitore dovrà predisporre un documento intitolato "Specifiche di dettaglio delle prove di collaudo dei servizi in ambiente di prova (*test bed*)" contenente almeno:

7.2.7.2. Architettura della piattaforma tecnica (TEST BED);

- il sistema di misura dei livelli di servizio e di generazione della reportistica;
- la modalità di svolgimento delle prove di collaudo.

Il Documento sopra descritto dovrà essere reso disponibile dal Fornitore entro 30 giorni lavorativi dalla richiesta di Consip/Agid. A partire dal 15esimo giorno successivo alla ricezione della documentazione di cui sopra da parte di Consip/AGID, il fornitore deve rendersi disponibile all'avvio dei collaudi.
Consip/Agid si riservano di chiedere adeguamenti al documento di cui sopra, che il fornitore dovrà recepire e formalizzare in una nuova versione del documento entro 15 giorni dalla richiesta.
Il buon esito del collaudo sarà comunicato da Consip/Agid mediante verbale, sottoscritto anche dal Fornitore.
Qualora dagli accertamenti effettuati in sede di primo collaudo, i servizi non risultassero conformi alle specifiche di dettaglio previste nelle prove di collaudo, il fornitore dovrà eliminare i vizi accertati entro i termini fissati dalla stazione appaltante, e comunque non inferiori a 5 (cinque) giorni lavorativi. Decorso detto termine, si potrà procedere ad una seconda prova di collaudo in *test bed*.
Consip/AGID si riservano di effettuare attività di verifica sui servizi secondo le modalità ed i tempi sopra espressi anche nel corso della fornitura, con l'obiettivo di accertare la permanenza dei requisiti richiesti.
Consip/AgID si riservano la facoltà di svolgere ispezioni sulle strutture Help Desk, sui Centri Servizi del Fornitore Aggiudicatario, o degli eventuali sub-fornitori, con un preavviso minimo di 3 (tre) giorni lavorativi, per verificare il permanere, nel periodo di vigenza contrattuale, dei requisiti richiesti.

7.2.6.1. **Collaudo di configurazione**

In seguito alla stipula del Contratto Esecutivo, l'Amministrazione contraente potrà richiedere prove di collaudo atte a verificare la conformità di ogni singolo servizio contrattualizzato rispetto a:

- “Piano dei fabbisogni”, redatto dall’Amministrazione contraente;
- “Progetto dei fabbisogni”, redatto dal Fornitore;
- Specifiche e requisiti dei servizi, contenuti nel Capitolato Tecnico.

A tal fine, il Fornitore deve obbligatoriamente effettuare quanto segue.
Il Fornitore deve fornire il supporto all’Amministrazione contraente in tutte le attività necessarie alle suddette prove di collaudo.
Il Fornitore deve consegnare (entro i tempi previsti nel Progetto dei Fabbisogni) all’Amministrazione un documento intitolato “Specifiche di dettaglio delle prove di collaudo” che descrive la tipologia delle prove di collaudo previste e la pianificazione temporale delle stesse.
Il Fornitore deve altresì impegnarsi, qualora richiesto dall’Amministrazione, a svolgere ulteriori prove integrative. L’Amministrazione può procedere, a sua discrezione, ad un collaudo a campione.

7.3. Modalità di subentro (phase in)

A partire dalla data di stipula del Contratto Esecutivo, il Fornitore potrà richiedere il supporto dell’Amministrazione contraente o di terzi da essa designati al fine di permettere al proprio personale la presa in carico delle attività di fornitura e di acquisire le conoscenze necessarie al corretto svolgimento dei servizi richiesti per il periodo definito congiuntamente all’Amministrazione contraente nel piano di migrazione; le attività di phase in non comporteranno ulteriori oneri per l’Amministrazione contraente.
L’attività potrà consistere, ad esempio, in riunioni di lavoro, rilevazione delle configurazioni in essere sui vari sistemi, esame della documentazione esistente (es. elenco degli asset informatici, catalogo dei sistemi e delle applicazioni, documentazione relativa agli sviluppi in corso, base dati dei contratti con terzi, etc.) con assistenza di personale esperto, affiancamento nell’operatività quotidiana condotta dall’eventuale fornitore uscente. Qualora la documentazione disponibile risultasse non aggiornata e/o incompleta, tutto ciò dovrà risultare in modo dettagliato in un verbale attestante il completamento del passaggio di consegne. Tale verbale dovrà essere sottoscritto dai due Fornitori, l’uscente e il subentrante (ovvero tra l’Amministrazione contraente e l’Aggiudicatario) e consegnato all’Amministrazione.
Durante le attività di *training on the job* la responsabilità delle operazioni continuerà ad essere in capo al Fornitore uscente, se presente. Le modalità di fruizione e la relativa pianificazione di tale addestramento dovranno essere concordate con

l'Amministrazione contraente, anche sulla base di eventuali proposte che il Fornitore effettuerà nella Relazione Tecnica.
Per tutto il periodo di affiancamento di inizio fornitura (*phase in*), il Fornitore Aggiudicatario non percepirà alcun corrispettivo.
Eventuali attività tecniche di *phase in* correlate all'installazione o alla migrazione di sistemi o di loro componenti dovranno essere svolte secondo quanto descritto nei seguenti paragrafi.

7.3.1. Modalità di attivazione

La presente sezione definisce le modalità di attivazione dei servizi di ogni Contratto Esecutivo. Il fornitore deve obbligatoriamente eseguire quanto di seguito descritto.
In generale, il Fornitore aggiudicatario del Contratto deve effettuare tutte le attività descritte nel paragrafo sia nel caso di migrazione di un'Amministrazione da servizi preesistenti, sia nel caso di realizzazioni o presa in carico ex novo.
Nel caso in cui l'Amministrazione fruisca di servizi preesistenti, il Fornitore deve esplicitamente prevedere, congiuntamente con l'Amministrazione contraente, le procedure di attivazione necessarie a garantire il mantenimento dell'operatività durante le fasi di migrazione. Eventuali necessità di fermo dei servizi devono essere accuratamente definite dal Fornitore, approvate dall'Amministrazione e monitorate in modo da ridurre al minimo gli impatti sull'utenza di riferimento.
Si precisa inoltre che in fase di avvio dell'erogazione dei servizi, il Fornitore dovrà sottoscrivere un accordo di riservatezza che lo impegna a non divulgare nessuna informazione relativa all'Amministrazione contraente, alle sue infrastrutture informatiche e ai suoi dati.

7.3.2. Attività di installazione/Manutenzione

In relazione ad eventuali attività di installazione/manutenzione presso le sedi dell'Amministrazione, Il Fornitore dovrà obbligatoriamente definire, congiuntamente con l'Amministrazione contraente, il piano di installazione/manutenzione dei servizi, che dovrà rispettare i seguenti requisiti minimi:

- gli interventi dovranno essere effettuati in intervalli orari definiti dall'Amministrazione contraente, coerentemente con le proprie esigenze di operatività;
- l'operatività del servizio deve essere garantita anche durante la fase intermedia di test e collaudo;

- l'impatto delle operazioni di roll-out e installazione sulla normale operatività delle sedi dovrà essere ridotto all'essenziale.

Qualora un'operazione di installazione dovesse costituire causa di disservizio, il Fornitore dovrà adoperarsi per garantire il ripristino immediato della condizione preesistente (procedura di *roll-back*).

A partire dalla data di decorrenza del Contratto Esecutivo, il Fornitore dovrà procedere all'installazione secondo le modalità temporali previste dal Progetto dei Fabbisogni; per tale attività e per le eventuali successive attività di configurazione il Fornitore, congiuntamente con l'Amministrazione, dovrà:

- contattare il referente tecnico della sede,
- concordare le modalità ed i tempi di interventi on-site,
- effettuare una verifica del sito, se necessario,
- procedere alle specifiche attività di installazione e configurazione,
- partecipare alle attività di test ed emettere un verbale per collaudo eseguito con esito positivo.

7.3.3. Eventuali attività di migrazione funzionali alla presa in carico dei servizi

Nel caso in cui la presa in carico di un servizio richiedesse attività di migrazione, il Fornitore dovrà obbligatoriamente concordare con l'Amministrazione contraente un piano specifico, nel quale indicare obbligatoriamente gli interventi da eseguire e le relative fasce orarie. Tutti gli interventi eseguiti sulle piattaforme in esercizio dovranno obbligatoriamente essere effettuati al di fuori dell'orario di lavoro del personale delle Amministrazioni e, comunque, in intervalli orari definiti dall'Amministrazione coerentemente con le proprie esigenze di operatività.
Pur nel rispetto della continuità del servizio, il piano proposto dal Fornitore deve consentire il massimo parallelismo delle attività al fine di minimizzare i tempi di attivazione.
Il processo deve prevedere, ove applicabile, una fase di "parallelo operativo" che garantisca, in una determinata finestra temporale, la coesistenza dei servizi erogati dall'attuale Fornitore. Il parallelo operativo deve essere tenuto attivo per il tempo necessario a completare le attività di migrazione e verificare la corretta operatività dei nuovi servizi. Il pagamento dei corrispettivi per la fornitura dei servizi oggetto di migrazione decorrerà dalla data di collaudo positivo (verbale di collaudo) del servizio

ovvero dalla data di accettazione da parte dell'AmministrazioneModalità di transizione in uscita (phase out).

7.4 Modalità di Phase-out

Il phase out, o transizione in uscita, consiste nelle seguenti attività da considerarsi come requisiti minimi:

- "passaggio di consegne" in caso di servizi *on premise* e servizi *as a service* nei quali si gestiscano sistemi delle amministrazioni,
- "consegna dei dati dell'Amministrazione", negli altri casi (es. consegna dell'immagine delle macchine virtuali),
- "consegna della documentazione tecnica" completa e aggiornata allo stato dell'arte dei servizi.

Il Fornitore dovrà garantire, al personale dell'Amministrazione o a terzi da essa designati, un periodo di supporto alla transizione, almeno pari a 3 mesi, al fine di consentire il trasferimento del know-how sulle attività condotte e rendere l'eventuale prosecuzione delle attività quanto più efficace possibile.

Tale periodo di affiancamento sarà organizzato secondo modalità da concordare con l'Amministrazione contraente e potrà prevedere sessioni riassuntive, sessioni di lavoro congiunto, presentazioni, tavole rotonde, ecc.

Al fine di facilitare il trasferimento del know how, il Fornitore dovrà predisporre il Piano di Trasferimento, articolato in attività con l'indicazione di scadenze di inizio e fine, di responsabilità, di contenuti e risultati tali da rendere controllabile l'effettivo svolgimento del trasferimento di know how; il piano, che dovrà essere formalizzato nei tempi richiesti dall'Amministrazione, dovrà essere prodotto congiuntamente tra Fornitore Aggiudicatario (uscente) e nuovo Operatore Economico individuato dall'Amministrazione Aggiudicatrice/amministrazione contraente e mantenuto aggiornato per tutto il periodo di vigenza contrattuale.

In particolare, la durata della transizione in uscita dovrà avere durata massima pari a 3 mesi, e svolgersi indicativamente negli ultimi 3 mesi antecedenti la scadenza Contratto Quadro, ma si riserva ad ogni Amministrazione la facoltà di rientrare in possesso di dati e configurazioni anche al termine dei singoli Contratti Esecutivi, con modalità analoghe alla transizione in uscita descritta nel presente paragrafo.

Nel caso in cui il phase out si sostanziasse unicamente nella consegna dei dati dell'Amministrazione, il Fornitore dovrà produrre dati e copie delle macchine virtuali, delle configurazioni adottate nell'utilizzo degli strumenti funzionali o a supporto dell'erogazione dei servizi, utilizzando formati standard indicati dall'Amministrazione contraente.

In ogni caso, l'Amministrazione contraente si riserva la facoltà di pianificare la consegna, da parte del Fornitore, di copie di prova dei dati e delle macchine, da sottoporre a test.

8. Governance della fornitura

Nel presente capitolo si forniscono indicazioni sulle modalità di governo dei Contratti Quadro, applicabili a tutti i Contratti derivati dai Lotti di gara, che i Fornitori Aggiudicatari devono obbligatoriamente rispettare.
Eventuali specificità riguardanti singoli lotti sono chiaramente evidenziate.

8.1. Referenti

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

- **un Responsabile del Contratto Quadro**, che avrà la responsabilità di gestire e risolvere tutte le problematiche legate al corretto svolgimento del Contratto Quadro nei confronti di Consip.
- **uno o più responsabili dei Contratti esecutivi**, che avranno la responsabilità di gestire e risolvere le problematiche relative ai singoli Contratti esecutivi, come fatturazione, rispetto dei livelli di servizio, etc.
- per i servizi "on premise" **uno o più Responsabili tecnici** , che avranno la responsabilità di coordinare dal punto di vista operativo tutte le attività legate ai servizi oggetto del presente capitolato tecnico e di essere il punto di riferimento per l'attivazione di nuovi servizi. Il Responsabile tecnico dovrà inoltre coordinare tutte le attività e produrre resoconti periodici, da presentare per discussione durante i SAL con le Amministrazioni.
- Per i servizi remoti **un Responsabile dei Centri Servizi** che avrà il compito di coordinare tutte le attività necessarie alla erogazione dei servizi previsti, ivi comprese quelle relative alla sicurezza.

I SAL, da tenere con cadenza almeno trimestrale o su esplicita richiesta dell'Amministrazione contraente, riguarderanno almeno i seguenti argomenti:

- dettaglio delle attività svolte e quelle ancora da svolgere;
- eventuali problematiche insorte;
- questioni aperte di carattere strategico/metodologico da sottoporre all'attenzione dell' Amministrazione contraente.

A fronte di eventuali problematiche che dovessero presentarsi, il SAL dovrà comprendere anche le relative proposte di risoluzione e le decisioni prese.
Su richiesta dell'Amministrazione, il Responsabile del Contratto esecutivo ed il/i Responsabile/i tecnico/i per l'erogazione dei servizi parteciperanno agli incontri con il Committente per comunicare gli aggiornamenti sullo stato dei servizi erogati e per condividere ogni eventuale azione correttiva necessaria al rispetto dei livelli di servizio (LdS) previsti. Tali incontri avverranno entro 10 giorni successivi alla richiesta, in data da concordare via mail tra le parti.

8.2. Valutazione risorse

Il Fornitore garantisce che tutte le risorse che impiegherà per l'erogazione dei servizi oggetto della fornitura, sia in fase di presa in carico dei servizi sia durante la fornitura stessa in caso di integrazioni e/o sostituzioni, rispondono ai requisiti minimi espressi dal presente capitolato.
A tal fine, il Fornitore, con le modalità ed i tempi previsti dal Contratto Esecutivo, sottoporrà i curricula vitae (CV) del personale dedicato alle attività presso l'Amministrazione contraente all'approvazione della stessa.
In ogni caso, per l'accettazione del personale proposto, l'Amministrazione contraente potrà procedere ad un colloquio di approfondimento per verificare la corrispondenza delle competenze elencate nel CV e il possesso delle certificazioni, laddove previste.
Per il personale ritenuto inadeguato, qualunque sia il ruolo ed il servizio impiegato, l'Amministrazione contraente procederà alla richiesta formale di sostituzione che dovrà avvenire seguendo le modalità ed i tempi previsti dal contratto.
In relazione al numero di risorse indicate nell'offerta per la valutazione dei punteggi inerenti le "Figure professionali – miglioramento anzianità nella funzione" e le "Figure professionali – presenza di certificazioni" (si veda lo specifico allegato per i singoli lotti) il fornitore aggiudicatario deve obbligatoriamente consegnare a Consip i relativi curricula entro la stipula del Contratto Quadro, tenendo conto che il curriculum di una medesima risorsa non può essere consegnato per più Lotti (si veda Lettera d'invito – Adempimenti per la stipula).

8.3. Aggiornamento dei prezzi

Per tutti i Contratti Quadro siglati con ogni aggiudicatario di ogni Lotto, è prevista una procedura di aggiornamento dei prezzi secondo le modalità di seguito descritte.

In particolare per i contratti dei Lotti 2, 3 e 4 si procederà ad un aggiornamento dei prezzi secondo quanto stabilito nel Contratto Quadro medesimo, al 30° (trentesimo) mese di validità del Contratto Quadro.

Per quanto concerne il Lotto 1, tale aggiornamento avverrà al 18° (diciottesimo) mese di validità del Contratto Quadro; Consip/Agid si riservano di procedere ad un ulteriore aggiornamento al 36° (trentaseiesimo) mese di validità del Contratto Quadro nel caso in cui il Contratto inerente il Lotto 1 venga prorogato, così come previsto nel contratto medesimo, per almeno ulteriori 12 mesi.

Per la definizione dei prezzi, Consip S.p.A. svolgerà, direttamente o tramite terzi, un'approfondita indagine atta a rilevare i migliori prezzi di mercato di servizi analoghi a quelli erogati dai fornitori assegnatari nell'ambito dei Contratti Quadro.

Nello specifico, Consip S.p.A. predisporrà un nuovo file "revisione.xls" originato dal file "Allegato 3 - Offerta economica Parte B" del Fornitore Aggiudicatario (cfr. Lettera di invito). Nel nuovo file le singole voci di prezzo saranno moltiplicate per i nuovi pesi che saranno individuati tenendo conto dei seguenti criteri:

- analisi delle effettive consistenze dei servizi acquisiti dall'insieme delle amministrazioni sottoscrittrici dei Contratti esecutivi pervenute a Consip/AgID;
- ipotesi di evoluzione del mercato e di utilizzo futuro dei servizi da parte delle amministrazioni;
- mantenimento della coerenza complessiva del listino prezzi.

Di seguito si elencano le varie fasi della procedura di revisione dei prezzi:

1) Per ciascuna delle tipologie di servizi saranno ricalcolati, attraverso il nuovo file "revisione.xls", i nuovi prezzi totali (P-n), utilizzando i prezzi di aggiudicazione offerti dal fornitore aggiudicatario nel file "Allegato 2 bis - Offerta economica Parte B.xlsx" e i nuovi pesi contenuti nel file;
2) Attraverso un'indagine di mercato saranno individuati i maggiori operatori nazionali ed internazionali operanti sul mercato italiano, compresi i fornitori assegnatari della presente gara. Per ognuno di tali operatori saranno raccolti i prezzi di servizi analoghi a quelli erogati dai fornitori assegnatari nell'ambito dei Contratti Quadro.
   I principali elementi alla base della valutazione dell'analogia saranno:
   - equivalenza qualitativa del servizio;
   - durata del contratto;
   - estensione territoriale dell'offerta;
   - dimensione della fornitura.

Attraverso un'opportuna metodologia presentata al Comitato che tenga conto degli elementi di analogia su elencati, i prezzi raccolti potranno essere corretti per renderli direttamente confrontabili con quelli in vigore nell'ambito dei Contratti Quadro.
Una volta individuati i migliori prezzi medi di mercato per ogni tipologia di servizio (P-m), nel caso in cui il P-n relativo ad una singola tipologia di servizio sia superiore al corrispondente P-m, i prezzi di quella tipologia di servizio saranno soggetti a revisione, il P-m diverrà il valore obiettivo della procedura di aggiornamento dei prezzi.
Il nuovo listino prezzi sarà oggetto di approvazione da parte del Comitato di Direzione Tecnica. I prezzi così ottenuti aggiornano il listino prezzi ed entrano in vigore con valore, eventualmente anche retroattivo, a decorrere dal mese successivo a quello in cui si è conclusa la rilevazione dei prezzi. Resta inteso che nessun prezzo contenuto nel listino prezzi potrà essere aumentato rispetto al valore offerto a gara.

8.4. Indicatori di qualità

Per ogni Lotto della presente fornitura, sono previsti Indicatori di qualità, descritti e dettagliati nell'Appendice 1 al Capitolato Tecnico.
Il Fornitore è tenuto, per l'intera durata dei servizi, a rendicontare gli Indicatori di qualità richiesti.
Durante l'intero periodo contrattuale ciascun indicatore di qualità potrà essere riesaminato in sede di Comitato; 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 indicatori di qualità che sono risultate non efficaci.
Il Fornitore si impegna a erogare i servizi tenendo conto delle modifiche richieste e a recepirle nel Piano della Qualità generale. Nella stesura del Piano della Qualità il Fornitore per ciascun Indicatore di qualità dovrà dettagliare le fonti dati utilizzate per la raccolta dei dati elementari nonché gli strumenti per l'elaborazione delle informazioni di dettaglio.

9. Orari di erogazione dei servizi

Sulla base della tipicità dei servizi previsti nell'ambito della presente fornitura, i Fornitori dovranno garantire i seguenti orari di servizio:

- H24, 7 gg su 7 per la disponibilità di risorse di calcolo, per le attività di monitoraggio e gestione incident relativamente ai seguenti servizi:
  - IaaS, PaaS, SaaS per il Lotto 1,
  - Servizi di Identity provider e I&AM, di firma digitale remota, sevizi di sicurezza di data loss/leak prevention, database security, web

application firewall e next generation firewall, secure web gateway e servizi di monitoraggio per il Lotto 2,

- Componenti infrastrutturali previsti nel Lotto 3, tra cui quelli per i servizi di Porta di dominio, web services, orchestrazione, open data, Big Data,
- Componenti Infrastrutturali per i servizi di Gestione Operativa per il Lotto 4,

- Per le attività di help-desk di ricezione chiamate con operatore: giorni feriali, dal lunedì al venerdì, dalle 8:30 alle 17:30 ; sabato (festivi esclusi) dalle 8:30 alle 14. Eventuali richieste di orari diversi da parte di singole Amministrazioni dovranno essere sottoposte all'approvazione del Comitato,
- Per tutti i servizi e le componenti di servizio che prevedono l'impiego di risorse professionali, giorni feriali, dal lunedì al venerdì, dalle 8:30 alle 17:30, prevedendo una flessibilità di 30 minuti in ingresso e in uscita del personale

Su quest'ultimo punto, in particolare, le Amministrazioni contraenti potranno modulare/modificare tale orario di erogazione dei servizi, dandone congruo preavviso ai Fornitori.

Eventuali estensioni dell'orario di servizio saranno formalizzate dall'Amministrazione contraente al Fornitore via posta elettronica.

Il preavviso minimo per le estensioni dell'orario di servizio sarà il seguente:

- nella stessa giornata lavorativa: 1 ora;
- disponibilità dei servizi il sabato, la domenica e/o nei giorni festivi: 4 ore antecedenti la fine dell'orario di lavoro della giornata lavorativa.

Qualora le richieste di estensione pervenissero nel periodo di preavviso prestabilito, esse non saranno soggette all'accettazione da parte del Fornitore.

Su richiesta dell'Amministrazione contraente, i Fornitori dovranno inoltre assicurare l'esecuzione di attività straordinarie, da eseguirsi al di fuori del normale orario di lavoro (in orario notturno e/o di sabato pomeriggio e/o nelle giornate festive) previa pianificazione e con preavviso di 2 giorni.

I volumi di attività da effettuarsi in reperibilità e extra orario saranno indicati dall'Amministrazione committente in fase di dimensionamento del servizio, a valle della stipula del Contratto Esecutivo.

Per attività fuori orario standard si prevede una tariffa maggiorata del 20% per profilo professionale coinvolto.

Le Amministrazioni potranno sottoporre al Comitato eventuali richieste per ulteriori esigenze in termini di orario di servizio.