BOZZA PRELIMINARE

Capitolato Tecnico

per l'affidamento dei servizi di Disaster Recovery degli Istituti assistenziali e previdenziali pubblici

BOZZA PRELIMINARE

1 DEFINIZIONI E GLOSSARIO DEI PRINCIPALI TERMINI USATI NEL DOCUMENTO E NEGLI ALLEGATI TECNICI O CONNESSI ALLA SOLUZIONE DI DISASTER RECOVERY

Asset: Sono tutte le risorse che costituiscono il patrimonio di un'organizzazione. Ne esistono tre tipi: asset fisico (edifici, apparecchiature); asset finanziari (moneta corrente, deposito bancari ed azioni); asset intangibili (reputazione).

Cold site: Centro di elaborazione d'emergenza che dispone dei componenti e delle infrastrutture elettriche di un sistema di produzione normale, ma non contiene i computer. Il sito è pronto per accogliere i computer quando occorre passare dal centro di calcolo principale a quello di riserva, in caso di disastro.

Condizione di emergenza: l'interruzione nell'operatività dei sistemi informativi localizzati nei rispettivi siti primari, che viene formalmente attivata con la "Dichiarazione di disastro" da parte del singolo Istituto e che permane fino al ripristino del sito primario con "Dichiarazione di fine emergenza" da parte dell'Istituto stesso.

(CO) Continuità operativa: Insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale. Include il **Disaster Recovery**.

Copia dei dati (Data Mirroring): Un processo con cui dati ritenuti critici vengono copiati in un'altra locazione, in modo che non vengano persi nell'evento di perdita di **Continuità Operativa**. Può essere utilizzata come soluzione di **Disaster Recovery** effettuando la copia remotamente. Esistono funzioni di copia dati a livello hardware e a livello software.

Crisi: Un evento o una percezione che minaccia le operazioni il personale, il valore dell'azienda, il nome, la reputazione e/o gli obiettivi strategici di una organizzazione.

Disaster Recovery: Insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso.

Disastro: Una calamità improvvisa e non pianificata che causa gravi danni o perdite. Tipicamente implica l'inizio del trasferimento dal sito primario al sito alternativo secondario di DR-NCUB.

NCUB: Nuovo Centro Unico di Backup, il un sito alternativo di Disaster Recovery geografico, nel territorio italiano, che sia in grado, in caso di disastro e/o di indisponibilità che colpisca i siti primari degli Istituti aderenti, di garantire l'accesso, anche contemporaneo, di tutti gli Istituti nel rispetto dei tempi di ripristino e ripartenza previsti;

Vecchio CUB: il Centro Unico di backup, che ha costituito il sito alternativo di recovery nella soluzione di Disaster Recovery precedentemente fruita dagli Istituti previdenziali, in ambito metropolitano;

Piano di Disaster Recovery: Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito, in genere, di una organizzazione.

Politiche di sicurezza: Costituiscono l'insieme dei principi, norme, regole, consuetudini che regolano la gestione delle informazioni di una organizzazione in termini di protezione e distribuzione. Si possono classificare in politiche di alto livello e funzionali.

Requisiti di sicurezza: Esprimono ciò che si intende per sicurezza: riservatezza,integrità e disponibilità.

Ripristino: Attività che consiste nel riportare un sistema al suo stato precedente ad un disastro o ad una condizione di emergenza, con riattivazione del sistema informativo primario. Nel caso di perdita di dati, permette di rigenerarli come erano prima dell'evento, in genere partendo da un backup.

RPO: Recovery Point Objective, indica la perdita dati tollerata Recovery Point Objective (RPO): rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e,

conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso.

RTO: Recovery Time Objective, indica il tempo di ripristino del servizio: è la durata di tempo e di un livello di servizio entro il quale un business process ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili.

SPC: Sistema Pubblico di Connettività (artt. 73 e segg. Del D.Lgs 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale"); è definito come l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della Pubblica Amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.

Storage Area Network (SAN): Rete ad alta velocità che consente di creare delle connessioni dirette tra i dispositivi hardware di memorizzazione dei dati e i server connessi in rete.

Tracciabilità: Azione continua di registrazione delle azioni svolte da un soggetto identificato univocamente; il termine inglese corrispondente è accountability.

Unità di Crisi: Un definito numero di ruoli e responsabilità per realizzare l'organizzazione del **Piano di Gestione Crisi**.

Warm site: A differenza dell'**hot site**, è un sito alternativo che non prevede un'infrastruttura completa. La configurazione include di solito le connessioni alle reti, le unità disco, le unità nastro ma non i computer.

2 INTRODUZIONE

Il presente documento, assieme agli allegati specifici dei singoli Istituti, descrive quanto necessario per la formulazione di una offerta per la progettazione, la realizzazione e l'erogazione dei servizi necessari alla fornitura di una soluzione di Disaster Recovery che evolva l'attuale soluzione degli Istituti previdenziali ed assicurativi, quale delineata nel presente capitolo e meglio descritta negli allegati 4, 5, 6 e 7 del presente documento, da un ambito attualmente metropolitano ad una soluzione di Disaster Recovery geografico.

2.1 L'attuale soluzione di Disaster Recovery: il Centro Unico di Backup

Allo scopo di proteggere i sistemi informativi da eventi disastrosi o da malfunzionamenti che possono causare la loro indisponibilità prolungata, è stato costituito un centro comune di Disaster Recovery (DR) denominato Centro Unico di Backup (CUB), atto a garantire la continuità operativa dei sistemi primari degli Istituti previdenziali ed assicurativi denominati anche Istituti aderenti) attraverso la disponibilità di servizi, risorse professionali e strumentali e tecnologie tali da poter gestire situazioni di prolungata indisponibilità dell'infrastruttura informatica. La soluzione tecnica finora adottata ha permesso di soddisfare le seguenti principali esigenze:

- proteggere i sistemi informatici da eventi disastrosi;
- tutelare il patrimonio di dati degli Istituti;
- prepararsi ad una corretta gestione delle emergenze;
- mettere a fattore comune risorse professionali, economiche e strumentali, anche nell'ottica della razionalizzazione della spesa informatica.

2.2 Descrizione della struttura della soluzione di continuità operativa adottata nell'ambito del CUB

Il sito attualmente utilizzato come Centro Unico di Backup è localizzato nella zona metropolitana di Roma. I centri primari degli Istituti sono ubicati in Roma.

Gli Istituti aderenti possono attivare i sistemi di recovery del CUB a seguito di indisponibilità prolungata dell'infrastruttura ICT, anche contemporanea, degli ambienti di esercizio sia a seguito di un evento distruttivo che colpisca il centro primario, tale da renderlo inoperativo per settimane o mesi, sia in caso di switch-over ovvero in occasione di lavori di manutenzione ordinaria e straordinaria dello stabile o degli impianti tecnologici del centro primario che richiedano lo spegnimento dei sistemi di esercizio.

L'architettura delle soluzioni degli Istituti, dati i vincoli di RTO (*Recovery Time Objective*) e RPO (*Recovery Point Objective*), prevede il mirroring dei dati, a disco e a nastro, utilizzando tecniche sincrone o asincrone di copia dati, sfruttando la larghezza di banda offerta da collegamenti in rete ottica metropolitana dedicati al CUB (che prevede ridondanza di percorsi per eliminare potenziali "*single point of failure*" nella componente TLC). La soluzione si avvale di tecniche operative e strumentali, hardware e software, che garantiscono la congruità e la consistenza dei dati. E' al momento adottata anche una soluzione che prevede la produzione di copie a nastro e il loro successivo trasporto e conservazione presso il CUB (soluzione a freddo).

Gli Istituti aderenti al CUB hanno determinato, sulla base delle rispettive esigenze operative, sia il tempo richiesto per il ripristino dei sistemi informatici (RTO - Recovery Time Objective) sia la massima perdita temporale dei dati (RPO - Recovery Point Objective). In linea con detti prerequisiti prestazionali sono state realizzate le idonee soluzioni tecnologiche e organizzative.

In linea generale, il tempo di riattivazione dell'infrastruttura informatica è previsto essere inferiore alle 4 ore, mentre la perdita dei dati è tendente a zero.

Per poter ottenere questo risultato, il CUB dispone di tutta la potenza elaborativa richiesta per la riattivazione dei servizi non più erogabili dai sistemi di esercizio e dispone dei collegamenti di telecomunicazione necessari per lo scambio dati con la periferia. Le configurazioni e la

consistenza dei sistemi sono tali da non indurre degradi prestazionali apprezzabili in caso di loro utilizzo per l'esercizio.

Per la connessione con il CUB, l'architettura, prevede una soluzione di networking ottico ad alta velocità basata su tecnologia di tipo DWDM (*Dense Wavelenght Division Multiplexing*) che consente di estendere le connessioni tra apparati SAN e LAN a distanze geografiche e garantisce estrema affidabilità, capacità e qualità del servizio.

Per quanto riguarda i dati, essi vengono duplicati in tempo reale sugli apparati storage presenti presso il CUB, realizzandone così una copia che consente di contenere la potenziale perdita di informazioni entro i limiti previsti.

L'attuale fornitore garantisce presso il CUB la presenza di uno staff di risorse professionali che assicura un presidio operativo h24 7g/7 per la ordinaria gestione dell'infrastruttura informatica e tecnologica e che, in caso di dichiarazione di disastro del/dei Centri di esercizio o di switch-over dell'ambiente di esercizio, provvede all'attivazione dei sistemi di backup entro i tempi prestabiliti. E' previsto che il personale dell'Istituto interessato, una volta completate le attività di attivazione dei sistemi, assuma il controllo per riattivare le applicazioni di esercizio, adottando le proprie normali procedure di gestione e controllo dei sistemi.

In caso di disastro o di indisponibilità dei sistemi primari, la successiva conduzione e controllo dei sistemi viene effettuata direttamente dal personale del/degli Istituti, ciascuno per i propri sistemi, in quanto il CUB sarà a tutti gli effetti il Centro di esercizio per tutta la durata dell'emergenza.

La parte telecomunicativa è invece predisposta e gestita da società di telecomunicazioni per la connessione in rete ottica metropolitana e dai fornitori dei servizio SPC.

Per verificare la funzionalità e l'efficienza delle soluzioni tecniche adottate da un punto di vista tecnologico, infrastrutturale ed organizzativo, nonché per valutare la correttezza delle prestazioni erogate dal fornitore, sono stati svolti, in linea con quanto prescritto, test periodici per simulare le condizioni di indisponibilità del sito primario, per verificare la tempestività e la correttezza dell'attivazione dei servizi applicativi sul sito secondario, nonché, per testare, in caso di indisponibilità prolungata del sito primario, l'efficienza dei processi definiti dalle parti per l'attivazione e l'utilizzo del sito secondario e le modalità con le quali assicurare la migrazione del personale verso il CUB.

Per consentire il monitoraggio ed il controllo della fornitura, il fornitore dei servizi del CUB è tenuto a produrre con cadenza mensile le rilevazioni dello stato di avanzamento della fornitura, che riportano l'evidenza delle attività svolte, dei livelli di servizio rilevati nel mese e delle eventuali criticità emerse nell'erogazione dei servizi connessi alla soluzione di Disaster recovery degli Istituti.

2.3 Cenni sulle procedure e sulle strutture organizzative per la gestione del Disaster Recovery

Le procedure tecnico-organizzative da seguire per attivare le configurazioni di emergenza, così come i ruoli e le responsabilità sia del personale di ciascun Istituto che di quello dei fornitori, sono regolamentate da una serie di norme contenute nel Piano di continuità operativa. Per l'approntamento e l'attuazione di tali norme, ciascun Istituto ha individuato le funzioni/strutture interne ed esterne ritenute necessarie per la gestione dell'emergenza informatica, per la gestione del personale, nonchè per le comunicazioni esterne.

I processi decisionali sono guidati da un comitato interfunzionale di ciascun Istituto, denominato Comitato di Crisi, il quale si avvale di tutte le competenze interne ed esterne per la gestione e il superamento della condizione di crisi.

Il Comitato di Crisi è competente circa la pianificazione e l'attuazione degli interventi organizzativi e tecnologici per porre termine alla crisi e per riattivare, al termine dell'emergenza, i sistemi primari presso il Centro di esercizio originario oppure, ove ciò non fosse possibile, presso un nuovo sito.

Le fasi in cui si articola il processo di gestione della crisi sono, in linea di massima, le seguenti:

- rilevare lo stato di emergenza;

- dare il preallarme;
- attivare formalmente ed operativamente il piano di continuità operativa;
- gestire il rientro.

Vista la particolarità della soluzione, che vede la condivisione, da parte di più Istituti, del sito e delle infrastrutture del CUB, sono stati valutati i rischi derivanti dall'accesso alle medesime risorse da parte di più Istituti e predisposti appositi strumenti e procedure per gestire la possibile contemporaneità di accesso alle strutture del CUB. Allo stato attuale le soluzioni implementate non prevedono apparati informatici condivisi tra gli Istituti.

Nel caso in cui uno o più Istituti dichiarino lo stato di emergenza, il Comitato di Crisi dell'Istituto interessato comunicherà al Comitato di Crisi di ciascuno degli altri Istituti ed alla Segreteria Tecnica del CUB la situazione e la stima del tempo di permanenza presso il CUB. La comunicazione sarà fatta via telefono e/o e-mail.

2.4 Architettura Tecnologica

Nel CUB sono presenti diverse piattaforme tecnologiche, rispondenti alle esigenze di recovery di ciascuno degli Istituti ed ai rispettivi ambienti di esercizio.

Si rimanda agli allegati specifici, relativi a ciascun Istituto, per la descrizione di dettaglio delle configurazioni dei siti primari e delle soluzioni di Disaster Recovery richieste.

3 OGGETTO DELL'APPALTO

L'oggetto dell'appalto consiste nell'acquisizione dei servizi relativi ad una soluzione di Disaster Recovery che nel caso di eventi disastrosi/situazioni di indisponibilità prolungata che rendano inutilizzabili i siti informativi primari degli Istituti aderenti (INPS, INAIL, INPDAP), assicuri il ripristino e la riattivazione di detti S.I. primari attraverso una soluzione che sia in grado di garantirne la continuità di funzionamento anche a fronte di disastri in ambito metropolitano.
A tale scopo il fornitore dovrà assicurare, nel rispetto delle specifiche funzionali, tecniche e dei livelli di servizio descritti nel presente documento e nei suoi allegati:

1. le connessioni trasmissive, non rientranti nei servizi SPC, per garantire il collegamento fra i siti primari ed il sito di Disaster Recovery – denominato anche Nuovo Centro Unico di Backup (per brevità NCUB) necessario al costante allineamento dei dati e delle configurazioni di produzione, funzionali al ripristino dei servizi ICT dei data center degli Istituti;
2. la messa a disposizione, gestione e manutenzione delle risorse elaborative e di storage, degli apparati attivi LAN e SAN e delle configurazioni necessarie alla soluzione di Disaster Recovery;
3. la messa a disposizione del sito di Disaster Recovery e delle infrastrutture attrezzate (posti di lavoro attrezzati e locali aggiuntivi per le operazioni di test e attività di riattivazione dei sistemi informatici primari);
4. l'assistenza operativa della soluzione di Disaster Recovery.

In merito al punto 2 le sole risorse di storage funzionali alla soluzione dovranno essere dedicate ed in uso esclusivo agli Istituti.

Nell'ambito dei servizi richiamati sempre al precedente punto 2, sarà cura del fornitore curare l'acquisizione, per conto di ciascuno degli Istituti, delle connessioni necessarie al collegamento del NCUB con le modalità ed alle condizioni tecnico economiche previste dai Contratti SPC nel rispetto di quanto previsto al successivo punto 5.4.

4 DECORRENZA, DURATA, PIANIFICAZIONE, AVVIO DEL SERVIZIO E GESTIONE DELLA FASE DI TRANSIZIONE DAL VECCHIO AL NUOVO CENTRO UNICO DI BACKUP

BOZZA PRELIMINARE

I servizi compresi nella soluzione DR-NCUB, dovranno essere erogati per ciascun Istituto, a partire dalla sottoscrizione del rispettivo contratto esecutivo – che verrà considerata "data di decorrenza" dei servizi - secondo quanto precisato nell'articolo 5 del contratto quadro e nell'articolo 5 dei contratti esecutivi di ciascuno degli Istituti aderenti e avranno termine alla scadenza del sessantesimo mese a far tempo da tale data di decorrenza.

Entro i primi 30 (trenta) giorni solari dalla sottoscrizione del contratto quadro il Fornitore e ciascun Istituto dovranno nominare i responsabili del contratto secondo quanto previsto dall'articolo 6 del contratto quadro.

Entro 60 (sessanta) giorni solari dalla sottoscrizione del contratto quadro il fornitore dovrà predisporre e sottoporre all'approvazione della Segreteria Tecnica di DigitPA e a ciascun Istituto, il Piano di progetto generale iniziale ed il Piano di Qualità della Fornitura secondo quanto prescritto nel prosieguo e con i contenuti di massima delineati nell'allegato 8 al presente Capitolato.

Nel Piano di Progetto generale presentato per il primo anno di vigenza del contratto (definito anche "Piano di Progetto generale iniziale" e che dovrà essere articolato in linea di massima tenuto conto di quanto richiesto sempre nel richiamato allegato 8 al presente Capitolato) dovranno essere analiticamente descritte i termini e le modalità di completamento delle attività che dovranno essere svolte sia da ciascun Istituto sia dal fornitore nella fase di avvio del servizio e di transizione dal vecchio al Nuovo Centro Unico di Backup.

Entro i primi cinque mesi dalla richiamata data di decorrenza sulla base del richiamato Piano di Progetto generale iniziale il fornitore si impegna a completare le attività di avvio del servizio e transizione al NCUB, fra cui le attività per la presa in carico della documentazione esistente, per la ricognizione della attuale soluzione di Disaster Recovery esistente, per la realizzazione e messa in esercizio della soluzione di Disaster Recovery geografica nel rispetto delle specifiche tecnico funzionali desumibili dai rispettivi allegati tecnici degli Istituti.

Entro i primi cinque mesi dalla richiamata data di decorrenza dei servizi, il fornitore si impegna altresì a predisporre e sottoporre all'approvazione della Segreteria Tecnica di DigitPA degli Istituti il Piano di Disaster recovery, di cui al successivo punto 4.1.1 e a progettare, realizzare e mettere in esercizio il Portale che sarà utilizzato per tutta la durata del contratto, per la gestione, il monitoraggio e l'esecuzione della fornitura.

Il Fornitore si impegna, comunque, nel periodo necessario alla definizione ed approvazione dei Piani a svolgere le attività previste senza impatti e interruzioni del servizio erogato dagli Istituti.

Le citate attività per l'avvio dei servizi ovvero:

- la ricognizione delle infrastrutture e delle procedure adottate nell'ambito delle attuali soluzioni di Disaster Recovery dei sistemi di ciascun Istituto;
- la presa in carico della documentazione esistente nonchè delle eventuali componenti di proprietà degli Istituti dettagliate nei relativi allegati;
- la ricognizione di tutte le specifiche caratteristiche di sicurezza fisica e logica richieste da ciascun Istituto;
- la predisposizione e presentazione del Piano di Disaster Recovery;
- la realizzazione e la messa in esercizio della soluzione di Disaster Recovery, comprensiva dell'infrastruttura CED, delle risorse elaborative, delle risorse di storage (esclusive per ciascun Istituto), nonché di tutte le componenti, degli spazi e delle postazioni messe a disposizione;
- la progettazione e l'implementazione della soluzione di DR geografico che porterà alla dismissione dell'attuale CUB e all'attivazione del Nuovo Centro Unico di Backup (NCUB);
- la disponibilità delle risorse elaborative, dello storage esclusivo e delle componenti ed apparecchiature, delle connessioni trasmissive necessarie alla soluzione di Disaster Recovery;
- la soluzione necessaria al collegamento del sito di NCUB alle sedi periferiche e geografiche di ciascuno degli Istituti in ambito SPC;
- le attività connesse alla fase di transizione dal vecchio al Nuovo Centro Unico di Backup,

dovranno, quindi, essere concluse entro cinque mesi dalla data di decorrenza dei servizi, con l'invio alla Segreteria Tecnica di DigitPA e a ciascuno degli Istituti, di apposita comunicazione di

completamento delle attività e di "pronti al collaudo", secondo quanto precisato nel successivo punto 6.

In allegato alla comunicazione da ultimo citata il fornitore, oltre al piano di collaudo, contenente la proposta delle verifiche e prove di collaudo che saranno svolte, dovrà inviare:

- una relazione dettagliata sullo stato della presa in carico e della ricognizione (l'esito delle ricognizione degli ambienti, delle configurazioni ed apparati relativi ai siti primari degli Istituti);
- una descrizione dettagliata della soluzione di DR del NCUB, del sito e delle componenti messe a disposizione;
- il Piano di Disaster Recovery di cui al punto 4.1.1. .

Resta ferma la facoltà di ciascuno degli Istituti di svolgere ulteriori verifiche rispetto a quelle proposte nel piano di collaudo e di decidere con quali modalità svolgere la verifica del completamento e dell'adeguatezza di tutte le attività richieste per il completamento della fase di avvio del servizio, di implementazione della soluzione di DR geografico e di transizione dal vecchio al NCUB.

Successivamente alla presentazione della comunicazione di "pronti al collaudo" le parti concorderanno il calendario dello svolgimento delle prove di collaudo, che saranno effettuate in contradditorio, verificando il rispetto dei termini e l'adeguatezza e completezza delle attività previste. L'esito positivo del collaudo sarà essenziale ai fini dell'inizio dei servizi di DR e delle procedure di pagamento dei corrispettivi dovuti.

Si applicherà quanto previsto dal successivo punto 6 e quanto disposto dagli articoli 8, 17 e 22 del contratto esecutivo di ciascuno degli istituti aderenti.

I servizi dovranno, pertanto, essere avviati il giorno successivo alla data del verbale che riporta l'esito positivo del collaudo.

Gli Istituti si riservano la facoltà, durante il periodo di transizione di effettuare in contraddittorio con il fornitore, dei test preliminari e propedeutici alle verifiche di collaudo, coinvolgendo ove necessario la Segreteria Tecnica di DigitPA, ai fini della efficiente attivazione dei servizi di Disaster Recovery affidati al fornitore aggiudicatario, al fine di verificare oltre al rispetto delle scadenze previste l'adeguatezza, la completezza e la rispondenza ai requisiti richiesti, a quanto previsto nel piano di progetto e negli allegati di ciascuno degli istituti.

Ai fini della gestione delle attività nella fase di avvio del servizio e di transizione dal vecchio al NCUB, gli Istituti si riservano di affiancare il fornitore aggiudicatario.

La descrizione degli ambienti, delle configurazioni ed apparati relativi ai siti primari degli Istituti dettagliati nei relativi allegati sono suscettibili, alla luce delle informazioni acquisite dal fornitore nel periodo di avvio del servizio di modifiche e/o integrazioni. L'esito della ricognizione effettuata dal fornitore sarà validato e, se approvato dai singoli Istituti, sarà utilizzato come descrizione aggiornata delle configurazioni dei sistemi per i quali devono essere erogati i servizi richiesti.

Il fornitore si impegna quindi a erogare i servizi previsti a parità di termini, costi e condizioni, anche qualora emergano nel periodo avvio del servizio, di ricognizione e presa in carico componenti hw e/o sw, ambienti, programmi, applicazioni e/o funzionalità che, ancorché non descritti e/o dettagliati, risultino comunque necessari alla soluzione di Disaster Recovery degli Istituti ed al corretto adempimento degli obblighi assunti nell'ambito del presente Capitolato, del contratto quadro e dei contratti esecutivi definiti per ciascun Istituto.

Il Piano di progetto generale ed il Piano di Qualità della fornitura, per gli anni di vigenza del contratto successivi al primo dovranno essere aggiornati almeno con cadenza annuale, inviati per conoscenza alla Segreteria Tecnica di DigitPA, e sottoposti all'approvazione di ciascuno degli Istituti entro i 30 (trenta) giorni solari precedenti all'inizio di ciascun anno secondo quanto previsto nel contratto quadro e nei contratti esecutivi, nonché nella tabella di cui al successivo punto 10.

Il Piano di Progetto Generale ed il Piano di Qualità della Fornitura potranno essere sottoposti a

revisione anche a fronte di rilevanti variazioni tecnico organizzative, ed essere sottoposti all'approvazione dell'Istituto/degli Istituti interessati, entro i 30 (trenta) giorni solari successivi alla richiesta di revisione, secondo quanto previsto nel successivo punto 10 e nell'articolo 7 del contratto esecutivo di ciascuno degli istituti aderenti.

4.1.1 Piano di Disaster Recovery; documentazione delle procedure operative

Il fornitore dovrà predisporre e sottoporre all'approvazione della Segreteria Tecnica di DigitPA e degli Istituti, in allegato alla comunicazione di avvenuto completamento delle attività connesse alla fase di avvio del servizio e di "pronti al collaudo", di cui al precedente punto 4, il Piano di Disaster Recovery di ciascuno degli Istituti aderenti che dovrà illustrare, secondo lo schema di massima delineato in allegato 7 al presente Capitolato, la soluzione di continuità operativa assicurata ed elencare le azioni da intraprendere prima, durante e dopo una situazione d'emergenza/indisponibilità del sito primario per assicurare la continuità del servizio reso dai sistemi informativi degli Istituti aderenti.
Il Piano dovrà contenere, a titolo esemplificativo e non esaustivo, per ciascun Istituto:

1) la pianificazione della gestione della crisi e delle attività da assicurare in condizioni di emergenza;
2) l'assegnazione di ruoli e responsabilità, con particolare riferimento alla gestione straordinaria da attuare in caso di disastro o indisponibilità prolungata dei siti primari;
3) la definizione delle modalità e dei termini di attivazione del personale e degli utenti dei sistemi informativi degli istituti;
4) il coordinamento del piano di test di Disaster Recovery;
5) la documentazione tecnica di ripristino, descrittiva delle strutture organizzative, delle procedure e della sequenza di attività da effettuare per la ripartenza ed il ripristino dell'operatività del Sistema informativo;
6) la descrizione delle modalità previste per assicurare l'assistenza al personale di ciascuno degli Istituti aderenti;
7) le modalità e i termini di rientro dalla situazione di emergenza.

Al fine di assicurare l'adeguatezza e l'efficacia delle operazioni in risposta a una situazione di emergenza o indisponibilità, il fornitore dovrà quindi pianificare le attività da svolgere e formalizzare le procedure operative da adottare, esplicitando i ruoli e le responsabilità.

Il Piano di Disaster Recovery di ciascuno degli Istituti aderenti dovrà essere aggiornato con cadenza annuale, inviandolo per conoscenza alla Segreteria Tecnica di DigitPA, e comunque revisionato in occasione di rilevanti variazioni tecnico organizzative, secondo quanto disposto dal successivo punto 10 e dall'articolo 14 del contratto esecutivo di ciascuno degli Istituti aderenti.

Il Piano potrà essere sottoposto a verifica ed eventuale revisione anche con cadenza semestrale secondo quanto previsto al successivo punto 13.

Si rimanda al relativo allegato 7 per la struttura e i contenuti che il fornitore dovrà rispettare nella redazione del piano di Disaster Recovery.

4.1.2 Strumenti a supporto della gestione e del monitoraggio dei servizi

Entro 60 (sessanta) giorni solari dalla sottoscrizione del contratto quadro, il Fornitore dovrà realizzare e mettere a disposizione del personale autorizzato degli Istituti un portale accessibile in modalità web per:

- inoltrare le richieste di intervento, configurazione e ripristino a fronte di malfunzionamenti e/o anomalie;
- inoltrare segnalazioni e comunicazioni inerenti alla fase di esecuzione della fornitura;
- monitorare anche da remoto, attraverso apposito sistema automatizzato, l'andamento dei servizi e dei livelli di servizio previsti;
- consentire il controllo e la tracciatura da remoto del traffico di rete e del funzionamento di tutti

gli apparati dedicati alla soluzione di Disaster Recovery per ciascun Istituto;
- rendere accessibili agli Istituti i deliverable, in particolare i report giornalieri e settimanali per il monitoraggio dei valori di RPO, le rendicontazioni dei servizi resi e dei livelli di servizio riscontrati, i piani di progetto e di qualità, i piani di Disaster Recovery;
- rendere accessibili i risultati dei test periodici.

Il Portale dovrà essere reso disponibile agli Istituti per tutta la durata contrattuale e dovrà essere localizzato nel sito di DR e fruibile dal personale di ciascun Istituto solo attraverso l'infrastruttura di rete dedicata alla soluzione di ripristino.
Il portale dovrà essere costantemente gestito, tenuto aggiornato e manutenuto per assicurare lo scambio delle comunicazioni, segnalazioni e informazioni attinenti alla fase di gestione del contratto, per garantire la verifica delle configurazioni del sito di DR e la presenza e accessibilità, da parte del personale degli Istituti, di sistemi di controllo dei livelli di servizio e di rendicontazione dei servizi resi.

Le attività di realizzazione e messa in esercizio del Portale dovranno essere concluse entro i previsti 60 giorni solari decorrenti dalla sottoscrizione del contratto quadro con l'invio alla Segreteria Tecnica di DigitPA e a ciascuno degli Istituti, di apposita comunicazione di completamento delle attività e di "pronti al collaudo" che dovrà riportare in allegato:
- il piano di collaudo, contenente la proposta delle verifiche e prove di collaudo che saranno svolte;
- la documentazione relativa al Portale di gestione dei servizi.

Successivamente alla presentazione della comunicazione di "pronti al collaudo" le parti concorderanno il calendario dello svolgimento delle prove di collaudo, che saranno effettuate in contradditorio, verificando il rispetto dei termini e l'adeguatezza e completezza delle attività previste. Si applicherà quanto previsto dal successivo punto 6 e quanto disposto dagli articoli 8, 17 e 22 del contratto esecutivo di ciascuno degli Istituti aderenti.

Il portale dovrà inoltre consentire, attraverso un sistema basato su autenticazione forte, la disponibilità di altre informazioni quali:
- gli esiti delle attività di test,
- le statistiche sull'andamento dei risultati delle misurazioni dei livelli di servizio,
- l'avvenuta presa in carico delle richieste di informazioni e delle segnalazioni di guasti e malfunzionamenti;
- l'avvenuta risoluzione dei guasti e/o malfunzionamenti e la notifica del ripristino delle funzionalità all'Istituto che ha segnalato i malfunzionamenti.

Le Parti si danno atto che comunque, fermo restando che il Portale rimarrà il primo canale di comunicazione e di interazione, nel quale dovrà essere assicurata la completa tracciatura di tutte le interazioni e attività svolte della fase di esecuzione della fornitura, nel Piano di Progetto sarà anche regolata la possibilità di provvedere allo scambio di comunicazioni, segnalazioni e informazioni attinenti alla gestione della fornitura anche attraverso apposite comunicazioni formali, attraverso messaggi di PEC ovvero attraverso comunicazioni ad un numero verde, messo a disposizione da parte del fornitore, per consentire, soprattutto ove il canale di collegamento al Portale non fosse disponibile, la possibilità di scambiare comunicazioni relative all'erogazione dei servizi anche attraverso i comuni dispositivi di telefonia mobile.
Il portale dovrà comunque mantenere traccia anche di eventuali comunicazioni, segnalazioni e scambi di informazioni effettuate non direttamente attraverso il Portale bensì attraverso apposite comunicazioni formali, attraverso messaggi di PEC ovvero attraverso comunicazioni al numero verde.

Il Portale dovrà quindi essere gestito dal Fornitore che si assume la responsabilità di garantire:
- la gestione del Portale;
- l'aggiornamento dei contenuti, la manutenzione delle componenti e la corretta alimentazione dei dati del Portale;

- la disponibilità in linea per gli Istituti delle informazioni di interesse;
- l'accesso agli utenti abilitati tramite credenziali di identificazione.

Il fornitore dovrà svolgere tutte le attività per garantire la continua disponibilità del Portale nel mese secondo quanto previsto in allegato 1 al presente Capitolato e dare evidenza attraverso lo stesso Portale dei tempi necessari nel mese per la gestione, l'aggiornamento e la manutenzione dello stesso Portale.
Ove non fosse avanzata alcuna riserva da parte di ciascuno degli Istituti, i tempi di gestione, aggiornamento e manutenzione del Portale saranno considerati come concordati ed accettati dagli Istituti e quindi esclusi dal calcolo della percentuale di disponibilità mensile prevista, ai fini della valutazione dell'adempimento e dell'eventuale calcolo della penalità.

Attraverso il Portale dovrà essere possibile avanzare richieste di intervento, segnalazioni, comunicazioni inerenti alla fase di esecuzione della fornitura.
Sarà cura del Fornitore implementare e realizzare il Portale, prevedendo un sistema che sia in grado di prendere in carico e tracciare tutte le richieste di intervento a fronte di guasti e malfunzionamenti, in particolare le richieste di manutenzione e assistenza o gli interventi di manutenzione avviati dal Fornitore nell'ambito delle attività di competenza.
Tutte le richieste di intervento e le segnalazioni dovranno essere tracciate attraverso il portale, al fine di consentire al personale di ciascuno degli Istituti di avere evidenza della data e ora di ricezione e presa in carico, dello stato delle attività svolte per far fronte alle richieste, dell'esito delle richieste di intervento, delle risposte alle comunicazioni formalizzate attraverso il Portale.

Ferma restando la facoltà di ciascun Istituto di definire congiuntamente col fornitore il livello di dettaglio delle informazioni da riportare sul Portale, per ciascuna segnalazione e richiesta di intervento a fronte di guasti, malfunzionamenti e/o anomalie dovrà essere data evidenza almeno delle seguenti informazioni:

- identificazione del problema o del malfunzionamento;
- modalità di ricezione;
- data e orario di ricezione;
- data e orario di inizio dell'intervento ;
- soggetto dell'Istituto che ha fatto richiesta ;
- soggetto che ha preso in carico la gestione del malfunzionamento;
- descrizione del malfunzionamento da parte dell'utente;
- descrizione della diagnosi e della soluzione adottata dal personale che gestisce il malfunzionamento

Come si è già avuto modo di evidenziare nel precedente punto 4 in merito alla fase di avvio dei servizi, il Fornitore dovrà documentare la struttura e le caratteristiche del Portale nonché le modalità di acquisizione dei dati e di monitoring degli indicatori dei servizio assicurando che il sistema di monitoring garantisca l'accuratezza, la completezza e la coerenza dei valori relativi alla elaborazione del calcolo dei livelli di servizio, periodicamente riscontrati.

5 DESCRIZIONE DELLA FORNITURA

5.1 Obiettivi e ambito della fornitura

Obiettivo della fornitura è assicurare, per ognuno degli Istituti tutte le attività necessarie alla replica dei dati, secondo quanto specificato per ciascuno degli Istituti aderenti nel relativo allegato e garantire la disponibilità e la ripartenza delle infrastrutture ICT necessarie al ripristino dei servizi e dei processi informatici, nel caso in cui si verifichino significative condizioni di emergenza.

Si definisce come condizione di emergenza l'interruzione nell'operatività dei sistemi informativi localizzati nei rispettivi siti primari, che viene formalmente attivata con la "Dichiarazione di disastro"

da parte del singolo Istituto e che permane fino al ripristino del sito primario con la "Dichiarazione di fine emergenza" da parte dell'Istituto stesso.

Il fornitore prende atto che nel presente Capitolato e nello schema di contratto relativo sono descritti i servizi e gli obblighi di carattere generale che dovranno essere rispettati per assicurare la soluzione di Disaster Recovery degli Istituti assistenziali e previdenziali pubblici, nonché per garantire la progettazione e l'implementazione della soluzione di DR geografico che porterà alla dismissione dell'attuale CUB e all'attivazione del NCUB.

Ciascuno degli Istituti provvederà con proprio contratto esecutivo a formalizzare e a precisare le prestazioni che il fornitore dovrà svolgere per assicurare l'erogazione dei relativi servizi.

Il ripristino dell'infrastruttura ICT dovrà avvenire:

- con un RTO massimo di 72 ore per ciascun Istituto richiedente il servizio di risorse elaborative;
- con un RPO di 5 minuti per le piattaforme che insistono su sottosistemi storage a disco con copia remota dei dati;
- con un RPO di 24 ore per dati a nastro che provengono da operazioni di backup.

Il mancato rispetto di detti obiettivi che rivestono il ruolo di indicatori e livelli di servizio della fornitura darà luogo all'applicazione delle relative penali secondo quanto indicato nell'allegato 1 al presente Capitolato e nei contratti esecutivi relativi a ciascun Istituto.

5.2 Requisiti e specifiche di erogazione dei servizi.

5.2.1 Obblighi e vincoli di carattere generale

Il fornitore si impegna ad assicurare la disponibilità di un sito alternativo di Disaster Recovery geografico, nel territorio italiano, che sia in grado, in caso di disastro e/o di indisponibilità che colpisca i siti primari, di garantire l'accesso, anche contemporaneo, di tutti gli Istituti al sito secondario, denominato "Nuovo Centro Unico di Backup", nel rispetto dei tempi di ripristino e ripartenza previsti nell'allegato 1 al presente Capitolato e richiamati nel precedente punto 5.1.

Detto sito dovrà posto ad una distanza minima di 200 km in linea d'aria da piazza Guglielmo Marconi, Roma.

Si rimanda per un maggior dettaglio agli allegati relativi a ciascun Istituto aderente per quanto attiene agli ambiti che devono essere coperti dalla soluzione di Disaster Recovery.

Il fornitore si impegna ad assicurare a ciascun Istituto i servizi necessari a permettere la riattivazione e il ripristino del proprio sistema informativo, garantendo anche in presenza di un evento catastrofico a carattere metropolitano che coinvolga l'area di Roma, l'accesso concomitante al servizio di DR da parte di tutti gli Istituti aderenti.

Il fornitore si impegna ad assicurare che ciascun Istituto aderente disponga presso il sito di DR di risorse di storage dedicate ovvero destinate in via esclusiva e senza alcuna forma di condivisione al singolo Istituto aderente per tutto il periodo di vigenza del contratto.

Per quanto riguarda le risorse elaborative diverse da quelle di storage la soluzione proposta potrà prevedere l'utilizzo di risorse non dedicate, ferme restando le garanzie specifiche sull'accesso al servizio espressamente richieste ed i livelli di servizio definiti nell'allegato 1 al presente Capitolato e richiamati nel precedente punto 5.1.

Per quanto attiene ai requisiti che il sito e le infrastrutture tecnologiche devono possedere, il Fornitore è tenuto a garantire che sia il sito che gli impianti siano stati progettati tenendo conto delle esigenze di continuità e manutenibilità dei moderni data center, garantendo:

– l'assoluta sicurezza del sito, ossia l'adozione di soluzioni in linea con lo stato dell'arte, dell'evoluzione tecnologica e della normativa vigente al riguardo, assicurando la protezione da accessi non autorizzati, la presenza di gruppi di continuità che garantiscano l'erogazione dell'elettricità senza interruzioni, la presenza di dispositivi antincendio e antiallagamento

nonché il rispetto dei requisiti richiesti nell'allegato 1 al bando di gara;
- la *fault tolerance* (letteralmente tolleranza ai guasti) con possibilità di isolare l'apparato in fault e provvedere alle riparazioni e/o alla sostituzione delle componenti guaste, senza pregiudicare la continuità delle funzionalità e del servizio erogato;
- la disponibilità a soddisfare le eventuali esigenze di crescita secondo le modalità previste al successivo punto 13, nel presente Capitolato e negli articoli 22, 23 e 25 dello schema di contratto esecutivo di ciascuno degli istituti.

Il fornitore si impegna a predisporre le opportune misure di protezione logiche e fisiche per proteggere i dati, contenuti negli apparati storage dedicati alla soluzione di DR, da accessi non autorizzati.

Nell'ambito del servizio, il fornitore dovrà, più in particolare:
- pianificare adeguatamente le attività da svolgere per assicurare il funzionamento della soluzione di Disaster Recovery (DR) di ciascuno degli Istituti aderenti;
- supportare gli Istituti nel definire i ruoli, le competenze e le responsabilità sia del personale degli Istituti aderenti sia del personale del Fornitore per ciascuna delle attività previste per assicurare la soluzione di DR;
- verificare costantemente nell'erogazione dei servizi la capacità della soluzione di DR implementata di rispondere efficacemente alle situazioni di emergenza e/o indisponibilità;
- garantire il costante allineamento della soluzione di DR rispetto all'evoluzione del sistema informatico e della struttura organizzativa degli Istituti aderenti;
- valutare costantemente l'aggiornamento tecnologico, l'adeguatezza delle risorse, delle componenti, degli accorgimenti e delle procedure messe a disposizione per assicurare il ripristino dell'operatività in occasione delle verifiche e dei test periodici (previsti per la simulazione delle situazioni di indisponibilità del sito primario di ciascuno degli Istituti aderenti);
- identificare, rendere evidenti agli Istituti ed attuare le eventuali misure di adeguamento e/o miglioramento (interventi di tipo tecnologico, organizzativo, procedurale e/o formativo e di comunicazione) di cui emergesse la necessità nel corso dell'erogazione dei servizi per assicurare l'adeguatezza e l'aderenza della soluzione di DR a fronte di rilevanti variazioni tecnico- organizzative;
- svolgere tutte le attività necessarie alla replica dei dati, secondo quanto specificato per ciascuno degli Istituti aderenti nel relativo allegato;
- svolgere le attività di verifica periodica del corretto dimensionamento e funzionamento della soluzione attraverso attività di manutenzione costante della soluzione di DR implementata e lo svolgimento delle previste sessioni di test;
- provvedere alla manutenzione delle soluzioni di DR, predisponendo e sottoponendo all'approvazione di ciascuno degli Istituti i piani di continuità, le rendicontazioni e i deliverable meglio dettagliati nel prosieguo e riepilogati al successivo punto 10;
- provvedere almeno una volta all'anno, in data da concordare con gli Istituti secondo le modalità di comunicazione e tracciatura definite nell'ambito del Piano di Progetto, un workshop finalizzato all'aggiornamento delle tematiche inerenti la sicurezza e le misure di Disaster Recovery e Continuità Operativa secondo un ordine del giorno concordato sempre con gli Istituti.

Il fornitore si impegna a mettere a disposizione degli Istituti ai fini dell'erogazione dei servizi personale che deve utilizzare la lingua italiana, per tutte le comunicazioni comunque formalizzate anche attraverso il Portale di gestione della fornitura, dotato di esperienza professionale con skill adeguato allo svolgimento delle attività di assistenza operativa, manutenzione della soluzione e supporto richieste, assicurando almeno il mix di risorse professionali di seguito riportato:

Figura professionale	% di effort per ciascuna tipologia di figura professionale
Sistemista	25
Operatore	75

Poiché la tipologia di contratto di lavoro subordinato meglio garantisce da un lato la qualità del servizio, dall'altro la continuità nello svolgimento delle attività e il mantenimento del Know how indispensabile alla corretta erogazione dei servizi, prevenendo un eccessivo "turn over" per effetto della "fidelizzazione" del personale dipendente, si richiede che almeno il 60% del team costituito per i servizi di DR sia composto da figure professionali presenti nell'organico del fornitore e assunte con contratti di lavoro a tempo indeterminato.

A tal fine il Fornitore si impegna ad indicare nel Piano di Progetto:

- la struttura organizzativa;

- i nominativi delle risorse messe a disposizione per l'erogazione di tutti i servizi e la ripartizione delle stesse nelle varie attività;

- la percentuale delle risorse messe a disposizione, presenti nell'organico e assunte con contratti di lavoro a tempo indeterminato.

Il fornitore si impegna ad inviare in allegato al Piano di Progetto generale (sia a quello iniziale sia nei Piani di progetto annuali, richiamati al precedente punto 4, al successivo punto 10 e negli atti negoziali che disciplinano l'esecuzione dei servizi) i curricula del personale che sarà tenuto allo svolgimento delle attività, con indicazione dei profili professionali, delle esperienze pregresse e soprattutto delle esperienze maturate in iniziative di Business continuity e o Disaster Recovery.

Il fornitore si impegna altresì ad assicurare, la stabilità e la continuità nel periodo di vigenza del contratto del Responsabile del contratto, del team e più in generale delle figure professionali che si interfacciano con gli istituti interessati, garantendo che il Responsabile del contratto e ciascuna risorsa professionale non sia sostituita salvo i casi di comprovata forza maggiore, per più di due volte nel corso della vigenza del contratto; si impegna anche ad osservare per i casi di sostituzione le disposizioni previste nell'articolo 16 di ciascuno dei contratti esecutivi degli Istituti interessati.

Nell'ambito dei servizi previsti e definiti nel presente Capitolato, senza ulteriori oneri aggiuntivi per gli Istituti aderenti, il fornitore dovrà altresì assicurare la disponibilità, il funzionamento e l'eventuale aggiornamento, allo stato della tecnologia e dell'arte, di tutti gli strumenti e prodotti che si rendano necessari a garantire la soluzione di DR e l'automazione di tutti i processi di recovery, il controllo continuo e da remoto della consistenza dei dati per le sessioni di mirroring.

Gli Istituti si riservano la facoltà di effettuare almeno una volta all'anno un test che preveda la simulazione di una situazione di disastro dei siti primari degli Istituti al fine di verificare il corretto ripristino e la riattivazione, presso il Nuovo Centro Unico di Backup, dei sistemi informativi, secondo quanto precisato al successivo punto 7.
I test effettuati non dovranno in alcun modo pregiudicare il servizio di copia remota dei dati, vale a dire non devono interrompere le garanzie di recovery richieste, garantendo accorgimenti e soluzioni che non pregiudichino la integrità e consistenza delle copie dei dati ospitate presso il Nuovo Centro Unico di Backup. Ulteriori requisiti specifici sono dettagliati negli allegati tecnici.

Il fornitore si impegna, comunque, ad accettare che ciascun Istituto, nell'ambito del proprio contratto esecutivo, si riservi di definire le condizioni che determinano la richiesta di erogazione del servizio di Disaster Recovery a proprio insindacabile giudizio.

Gli Istituti aderenti si riservano di rivedere nel corso della vigenza del contratto i servizi critici per i quali assicurare le soluzioni di Disaster Recovery verificando la compatibilità delle soluzioni adottate rispetto ai servizi erogati attraverso i sistemi informativi, operativi presso i rispettivi siti di produzione. Il Fornitore si impegna a mettere in atto tutte le iniziative a tal fine necessarie, definendo apposite proposte e ipotesi di revisione da sottoporre all'approvazione dell'Istituto che abbia manifestato la necessità di rivedere i servizi critici e/o la compatibilità della soluzione di DR e attuando le iniziative necessarie, ove possibile senza oneri aggiuntivi, salvo restando quanto previsto nei successivi punti 13 e 14 del presente Capitolato e quanto disposto negli articoli 22, 23 e 25 dei contratti esecutivi degli istituti.

5.3 Le connessioni trasmissive, non rientranti nei servizi SPC, per garantire il collegamento fra i siti primari ed il sito di Disaster Recovery necessario al costante

allineamento dei dati e delle configurazioni di produzione funzionali al ripristino dei servizi ICT dei data center degli Istituti

Il fornitore si impegna a garantire la connettività necessaria a sostenere il traffico dati tra i centri primari degli Istituti e il Nuovo Centro Unico di Backup geografico, prevedendo un doppio collegamento con instradamento totalmente diversificato per ogni tratta e per ciascuno dei siti dei data center degli istituti. Tale traffico comprende quello indotto dalla replica dei dati a disco e a nastro previsti dalla soluzione e quello relativo all'allineamento e controllo delle configurazioni di ripristino.

I collegamenti e gli apparati attivi che realizzano tale infrastruttura di interconnessione tra i siti devono essere realizzati evitando single point of failure e quindi prevedendo ridondanza di apparati e protezione del percorso.

La capacità di trasporto e le prestazioni trasmissive dovranno essere dimensionate tenendo conto dei dati di picco in scrittura stimati da ogni Istituto e descritti nei rispettivi allegati nonché tenuto conto dei vincoli di RPO predefiniti.

Il fornitore dovrà quindi assicurare la messa a disposizione e la manutenzione di tutte le componenti dirette a garantire la connettività fra i sistemi primari ed il sito del Nuovo Centro Unico nl rispetto di quanto previsto nell'allegato 9 (che attiene alla componente TLC e ai requisiti di banda richiesti per le soluzioni di DR)

5.4 Le connessioni SPC e la gestione dei rapporti con i provider SPC

Ai fini della funzionalità della soluzione ed in particolare, ai fini del ripristino della connettività geografica di cui ogni Istituto dispone sia con le proprie sedi periferiche, sia con terze parti, il fornitore si impegna a:

- 1) garantire la connettività necessaria a sostenere il traffico dati tra i centri primari degli Istituti e il Nuovo Centro Unico di Backup (NCUB) geografico;
- 2) acquisire, per conto di ciascuno degli Istituti (ad eccezione dell'INAIL) le soluzioni necessarie al collegamento delle sedi periferiche e geografiche o di terze parti al sito del Nuovo Centro Unico di Backup, alle condizioni tecnico economiche previste dai Contratti per i servizi di connettività SPC ed in linea con i requisiti di cui agli allegati 4, 5 e 6;
- 3) svolgere, per conto di ciascuno degli Istituti, il ruolo di interfaccia nei confronti dei provider SPC ai fini della gestione e dell'eventuale aggiornamento del piano dei fabbisogni nonché ai fini della gestione e del controllo del funzionamento della soluzione e delle connessioni SPC;
- 4) dare evidenza nei documenti di pianificazione e rendicontazione della fornitura delle attività svolte per assicurare il ruolo di interfaccia nei confronti dei provider SPC, per conto di ciascuno degli Istituti, ai fini:
- a) della gestione e dell'eventuale aggiornamento del piano dei fabbisogni;
- b) della gestione e del controllo del funzionamento della soluzione e delle connessioni SPC, evidenziando ai competenti provider SPC eventuali malfunzionamenti, problemi ed anomalie riscontrate eventualmente nel corso della fase di esecuzione dei servizi ovvero in occasione dello svolgimento dei test periodici previsti;
- 5) assicurare sul Portale di gestione della fornitura (di cui al punto 4.1.2) la tracciatura dello stato degli interventi svolti dai competenti provider SPC per la risoluzione degli eventuali malfunzionamenti, problemi ed anomalie riscontrate;
- 6) ospitare presso il NCUB degli Istituti gli apparati di collegamento SPC.

Per quanto attiene ai collegamenti SPC da acquisire secondo quanto richiamato al precedente punto 2), nel caso in cui nel corso di vigenza del contratto si esaurisse la possibilità di accedere ai listini e alle forniture SPC, il Fornitore si impegna comunque ad acquisire analoghe tipologie di collegamenti e forniture che garantiscano la connettività delle sedi periferiche degli Istituti e di terzi che si collegano ai siti informativi primari nell'ambito delle caratteristiche tecniche definite sempre nei richiamati allegati 4, 5 e 6.

5.5 Il servizio di messa a disposizione, gestione e manutenzione delle risorse elaborative e di storage, degli apparati attivi LAN e SAN e delle configurazioni necessarie ad assicurare la soluzione di Disaster Recovery di ciascuno degli Istituti aderenti

Il fornitore dovrà assicurare la disponibilità, la gestione e manutenzione delle risorse elaborative, dello storage, esclusivo di ciascuno degli Istituti aderenti, e delle apparecchiature LAN e SAN, di tutte le componenti anche ridondate, necessarie alla soluzione di DR, dettagliate per ciascun Istituto nel relativo allegato, assicurandone il corretto funzionamento, provvedendo, in caso di guasto/malfunzionamento/anomalia, a ripristinarne la funzionalità anche eseguendo le necessarie riparazioni e sostituzioni.

Il fornitore prende atto che tutte le componenti, anche ridondate, necessarie alla soluzione di DR di ciascun Istituto dovranno essere verificate ed eventualmente confermate/aggiornate al termine del periodo definito per l'avvio del servizio, la ricognizione e presa in carico, come anticipato nel precedente punto 4 e successivamente tenute sotto controllo di anno in anno per tutto il periodo di vigenza del contratto.

Il Fornitore dovrà quindi per tutta la durata del contratto:

- assicurare la disponibilità delle risorse elaborative, dello storage esclusivo e delle componenti ed apparecchiature (inclusi i posti di lavoro richiesti e dettagliati nel relativo allegato 2), necessarie alla soluzione di Disaster Recovery;
- assicurare il corretto funzionamento delle apparecchiature e delle componenti Storage dedicate alla soluzione di Disaster Recovery di ogni Istituto, dettagliate nel relativo allegato;
- garantire la manutenzione preventiva, secondo le specifiche di ciascuna apparecchiatura;
- dotarsi di strumentazione in grado di rilevare in automatico dalle singole apparecchiature ogni tipo di guasto, malfunzionamento o anomalia, parziale e\o totale che provochi degrado di tutte le componenti, anche ridondate, del servizio DR;
- assicurare la tracciatura sul portale (di cui al precedente punto 4.1.2) di ogni tipologia di segnalazione di guasti e malfunzionamenti, sia rilevati automaticamente, sia rilevati dalle singole parti;
- effettuare attività di diagnosi locale o remota, e provvedere, ove necessario, alle riparazioni/sostituzioni necessarie al mantenimento o ripristino del buon funzionamento delle apparecchiature;
- effettuare ove richiesto, le attività necessarie alla pianificazione ed installazione delle modifiche e dei miglioramenti tecnici per elevare la qualità e la sicurezza delle apparecchiature;
- assicurare il costante aggiornamento allo stato della tecnologia e dell'arte, di tutte le componenti dedicate alla soluzione di Disaster Recovery, senza oneri aggiuntivi.

Il fornitore dovrà in particolare assicurare le attività di manutenzione, intervento e ripristino della funzionalità per assicurare il rispetto dei tempi di risoluzione e ripristino previsti a fronte di malfunzionamenti e anomalie delle connessioni trasmissive, delle apparecchiature, dei server e dello storage, nonché di ogni altra componente messa a disposizione nell'ambito della soluzione di Disaster Recover), sia che siano segnalate in automatico dai sistemi di controllo delle apparecchiature, sia che siano riscontrate dal personale del fornitore o richieste dal personale di ciascuno degli Istituti aderenti.
A fronte di guasti, malfunzionamenti e/o anomalie di tutte le componenti, anche ridondate, del servizio DR dettagliate per ciascun Istituto nel relativo allegato, il ripristino dovrà essere assicurato secondo quanto precisato nell'allegato 1 al presente Capitolato:

- entro 4 (quattro) ore solari dalla data e ora del momento della segnalazione - comunque formalizzata - nel caso in cui il malfunzionamento e/o l'anomalia si manifestasse in condizioni normali;
- entro 1 (una) ora solare dalla data e ora del momento della segnalazione - comunque formalizzata - nel caso in cui il malfunzionamento e/o l'anomalia si manifestasse in condizioni di emergenza.

Ai fini del calcolo dei tempi di ripristino, si considererà il tempo di arrivo delle segnalazioni comunque pervenute (la data e ora della segnalazione in automatico dai sistemi di controllo delle apparecchiature; la data e ora del riscontro da parte del personale del fornitore; la data e ora della richiesta di intervento da parte del personale di ciascuno degli Istituti aderenti).

5.6 La disponibilità del sito di Disaster Recovery e di infrastrutture attrezzate

Il fornitore si impegna ad assicurare la disponibilità di un sito di disaster recovery con le caratteristiche minime descritte nell'allegato 1 alle "modalità di presentazione" del bando di gara e dotato di:

- infrastrutture necessarie a ospitare il personale degli Istituti durante i collaudi, i test e le situazioni di emergenza;
- spazi per ospitare gli apparati SPC nonché per ospitare eventuali connettività ritenute necessarie dagli Istituti stessi per la propria operatività;
- spazi e connettività necessari ad ospitare i sistemi di proprietà degli Istituti, i cui dettagli sono riportati negli allegati di riferimento.

5.7 Il servizio di assistenza operativa alle soluzioni di Disaster Recovery degli Istituti aderenti

Sarà responsabilità del fornitore assicurare per tutta la durata del contratto, il servizio di assistenza operativa presso il sito di Disaster Recovery-NCUB, per 24 ore al giorno e per 7 giorni alla settimana, nonché la gestione e la manutenzione delle soluzioni adottate da ciascuno degli Istituti aderenti.

A tal fine il fornitore dovrà provvedere ad assicurare la presenza di idoneo e qualificato personale a presidio dell'infrastruttura e delle apparecchiature dedicate alla soluzione di Disaster Recovery garantendo (a titolo esemplificativo e non esaustivo):

- il presidio, la gestione e la manutenzione delle infrastrutture dedicate alla soluzione di Disaster Recovery;
- la manutenzione della soluzione realizzata;
- l'assistenza operativa in condizioni normali e di emergenza e durante l'esecuzione dei test periodici previsti per la verifica del corretto funzionamento delle procedure di DR e del corretto dimensionamento delle componenti connesse alla soluzione di Disaster Recovery degli Istituti, sia per la parte IT che TLC;
- il monitoraggio e la gestione delle risorse al fine di mantenere e ottimizzare i livelli di servizio;
- la disponibilità della configurazione di ripristino in caso di emergenza in accordo con i livelli di servizio;
- la garanzia del costante allineamento fra le copie dei dati del sito di Disaster Recovery e i dati del sistema informativo primario di ciascuno degli Istituti aderenti;
- la rendicontazione giornaliera e settimanale dei livelli RPO riscontrati attraverso il Portale di gestione della fornitura;
- la consegna, entro il primo giorno della settimana successiva a quella di rilevazione, della rendicontazione dei livelli di RPO giornalieri della settimana oggetto di osservazione;
- la definizione e il costante adeguamento delle procedure di Disaster Recovery;
- la predisposizione e l'aggiornamento del Piano di Disaster Recovery nonché della relativa manualistica;
- il supporto e l'assistenza per assicurare a ciascun Istituto il ripristino della normalità dalla condizione di emergenza e la ripresa dell'operatività del Sistema Informativo Primario;
- le attività per riportare i dati e le configurazioni dei sistemi dal sito di DR - NCUB, al sito primario, secondo quanto previsto nel Piano di Disaster Recovery;
- la predisposizione e formalizzazione dei deliverable e delle rendicontazioni previste.

5.7.1 L'assistenza operativa in condizioni normali

Il fornitore, per ciascuno degli Istituti aderenti, avrà il compito di assicurare il corretto funzionamento dei sistemi installati presso il sito di DR in condizioni di normale operatività del sito primario dell'istituto e la loro effettiva disponibilità secondo quanto stabilito nell'allegato relativo a ciascun Istituto.
Il servizio di assistenza operativa comprende essenzialmente e specificatamente le attività di presidio per la gestione operativa di tutti i sistemi ospitati nel sito di Disaster Recovery (NCUB).
Il servizio si svolgerà 7 giorni su 7, 24 ore al giorno, comprendendo, a titolo esemplificativo, le seguenti principali attività che il fornitore dovrà meglio dettagliare nel Piano di Progetto:

- il controllo del corretto funzionamento del sistema e della corretta esecuzione delle procedure automatiche, con l'obiettivo primario di implementare e gestire nel corso di durata del servizio funzionalità di monitoraggio e gestione degli allarmi relativi:
    - alle risorse hw e sw di base dei sistemi (dischi, memoria, processori, connessione di rete, SAN Fabric, …) sia messe a disposizione del fornitore, sia di proprietà di ciascuno degli Istituti aderenti;
    - allo stato dei prodotti di gestione mirroring e backup;
    - alla connettività tra i sistemi attivi nel sito di DR.
- Il monitoraggio via Web interface di tutte le funzionalità di mirroring;
- la pianificazione operativa delle attività schedulabili;
- la gestione delle risorse di sistema al fine di mantenere e ottimizzare i livelli di servizio;
- la fornitura dei deliverable e rendicontazioni previste.

5.7.2 Assistenza operativa in emergenza

Il fornitore, per ciascuno degli Istituti aderenti, avrà il compito di attivare correttamente e in ottemperanza ai livelli di servizio richiesti la configurazione di emergenza della soluzione di DR prevista, secondo quanto stabilito nell'allegato relativo a ciascun Istituto, assicurando altresì l' assistenza operativa ed il presidio, a supporto del personale dell'Istituto che è comunque responsabile della conduzione in esercizio dei sistemi, 7 giorni su 7, 24 ore al giorno.

5.7.3 Assistenza operativa in fase di test

Il fornitore dovrà assicurare lo svolgimento dei test periodici previsti per la verifica del corretto funzionamento delle procedure di Disaster Recovery come meglio specificato nel successivo punto 7.

6 TERMINI E MODALITA' DI SVOLGIMENTO DELLE VERIFICHE E DEI COLLAUDI

Ove fosse necessario, ed in particolare al termine del periodo iniziale di avvio del servizio, ricognizione, presa in carico, progettazione ed implementazione della soluzione di DR (di cui al precedente punto 4), nonchè a fronte delle attività svolte dal fornitore nel periodo di erogazione dei servizi, gli Istituti si riservano di procedere a verifiche e collaudi, per verificare l'adeguatezza e la conformità dei servizi erogati ai requisiti della fornitura.

Le operazioni di collaudo saranno convocate a seguito della comunicazione di completamento delle attività e di "pronti al collaudo". In via generale, gli Istituti si riservano la facoltà di coinvolgere, ove necessario, nelle attività di verifica e collaudo, le strutture di DigitPA, che ha il ruolo di supervisione e supporto definito nell'articolo 6 del Contratto Quadro.

La comunicazione di pronti al collaudo della fase di avvio e transizione di cui al precedente punto 4 dovrà essere inviata alla Segerteria Tecnica di DigitPA e a ciascuno degli istituti, attraverso il Portale e con le modalità di comunicazione e tracciatura previste nel Piano di Progetto di cui sempre al precedente punto 4.

Le operazioni di collaudo a seguito del completamento della fase di avvio e transizione dal vecchio al nuovo CUB dovranno essere iniziate entro i 20 giorni solari successivi alla comunicazione di

"pronti a collaudo" o nel diverso termine proposto nel Piano di Progetto Generale iniziale approvato.

Analogo termine sarà osservato per il collaudo e la verifica dell'attività di realizzazione del Portale, di cui al precedente punto 4.1.2.

Le operazioni di collaudo si svolgeranno in contraddittorio secondo quanto precisato nell'articolo 17 del contratto esecutivo di ciascuno degli Istituti aderenti. Il collaudo si considera positivamente superato qualora tutti i risultati siano positivi. Al termine delle operazioni di collaudo dovrà essere redatto apposito verbale sottoscritto dal personale delle parti che vi ha partecipato, con precisazione dell'esito del collaudo stesso.

Per quanto attiene al collaudo della fase richiamata al precedente punto 4, come precisato nell'articolo 17 del contratto esecutivo di ciascuno degli istituti aderenti, i servizi dovranno essere avviati il giorno successivo alla data del verbale che riporta l'esito positivo del collaudo.

In caso di esito negativo del collaudo, fatte salve le penali previste, il fornitore si impegna a svolgere ogni attività necessaria per risolvere i problemi evidenziati, restando a suo carico ogni onere derivante dalle attività suddette.

Il collaudo potrà essere reiterato una sola volta con le medesime modalità e termini del primo collaudo, secondo quanto previsto nell'allegato 1 al Capitolato.
In ogni caso, è da considerarsi equivalente al mancato superamento del secondo collaudo, la mancata o tardiva convocazione, da parte del fornitore, della nuova seduta per la ripetizione delle operazioni di collaudo, entro i termini previsti.

7 TERMINI E MODALITA' DI SVOLGIMENTO DEI TEST DI DISASTER RECOVERY

Il fornitore si impegna ad eseguire, almeno una volta l'anno, il test periodico di Disaster recovery previsto per simulare il funzionamento del Nuovo Centro Unico di Backup in caso di disastro del sito di produzione principale dell'Istituto, al fine di verificare che sia assicurato il corretto ripristino del funzionamento del sistema informativo del sito primario.
Il fornitore dovrà effettuare i test periodici previsti per la verifica della corretta funzionalità delle soluzioni adottate per garantire la soluzione di Disaster Recovery dei sistemi primari degli Istituti aderenti ed assicurare che i servizi erogati vengano costantemente mantenuti allineati all'evoluzione dell'architettura e dei servizi.
Il fornitore dovrà predisporre il test al fine di simulare una "vera" condizione di emergenza/di indisponibilità prolungata, ed al fine di non rischiare di compromettere i dati di produzione per l'effettuazione delle simulazioni, dovrà predisporre copie dei dati ad uso esclusivo della simulazione che saranno cancellate al termine delle prove.
Il Fornitore dovrà verificare e testare le procedure formalizzate per garantire, in condizioni di funzionamento normale del centro primario, le operazioni di allineamento dei due centri (copia remota dei dati, ecc.).

Gli Istituti si riservano la facoltà di chiedere la possibilità di effettuare il test congiuntamente .

In occasione dei test gli Istituti si riservano la possibilità di effettuare test di carico anche automatizzati (attraverso propri tools), ai fini della verifica della rispondenza delle risorse elaborative richieste dalle soluzioni dei singoli Istituti e messe a disposizione dal fornitore.

I test della soluzione di Disaster Recovery verranno svolti coerentemente alle soluzioni adottate da ciascuno degli Istituti e secondo quanto pianificato nel piano di progetto generale annuale.

Il Fornitore si impegna a mettere a disposizione degli strumenti per facilitare la gestione e la conduzione del test anche da remoto.

Il fornitore, nell'effettuazione dei test periodici di disaster recovery dovrà simulare uno scenario che

prevede l'indisponibilità di tutte le apparecchiature del sito primario e il ripristino nel sito di DR dell'infrastruttura ICT necessaria a erogare i servizi istituzionali.
DigitPA si riserva la facoltà di partecipare alle fasi di test e verifica della configurazione d'emergenza; a tal fine il Fornitore è tenuto a inviare la comunicazione della data di svolgimento del test anche alla Segreteria tecnica di DigtPA.

Il test dovrà essere articolato secondo le seguenti macro fasi, da definire operativamente nella documentazione che dovrà essere prodotta e manutenuta ai sensi del precedente punto 4.1.1:
- Messa a disposizione e verifica di tutta la documentazione procedurale e tecnica connessa ai servizi di DR;
- Attivazione e ripartenza dei sistemi nel sito di DR;
- Verifica delle funzionalità di base degli ambienti elaborativi;
- Verifica dell'allineamento e della congruità dei dati tra i siti primari di produzione e il sito di DR;
- Attivazione e verifica del corretto funzionamento del Middleware;
- Verifica dell'operatività infrastruttura di rete;
- Verifica della corretta distribuzione delle rotte IP tra gli apparati di rete;
- Verifica connettività tra il sito di DR e i siti primari;
- Attivazione dei sottosistemi applicativi;
- Test applicativi.

In generale l'attivazione dei sistemi nel sito di DR sarà basata su di una copia aggiuntiva dei volumi a disco da realizzare tramite le funzionalità di copia istantanea dei sottosistemi storage; ciò al fine di permettere l'effettuazione di test su copie aggiuntive dei dati (c.d. "dati a perdere") senza alterare i dati presenti sui volumi a disco costantemente allineati con quelli di produzione localizzati nei siti principali degli Istituti.
Ciò permetterà di effettuare i test senza mai sospendere le sessioni di copia remota e quindi senza abbassare il livello di protezione della soluzione.

Particolare cura dovrà essere posta durante l'effettuazione dei test affinchè, dal punto di vista del servizio erogato, il sito di DR sia isolato rispetto alla rete IP geografica degli Istituti ad esclusione delle sedi individuate per la realizzazione dei test applicativi.

Al fine di verificare la rispondenza delle caratteristiche di affidabilità delle infrastrutture del data center espressamente richieste come requisiti (nell'allegato 1 alle "modalità di presentazione" del bando di gara), duranti i test gli Istituti potranno richiedere la simulazione della indisponibilità dell'infrastruttura tecnologica cosi come richiesta nel suddetto allegato.

Il fornitore si impegna a redigere e sottoporre all'accettazione di ciascun Istituto il verbale del test e il documento di tracciatura dell'esito delle prove effettuate entro il termine che sarà stato definito con l'Istituto nella documentazione dei criteri di svolgimento dei test.

Ciascun Istituto si riserva, di comunicare formalmente al fornitore la propria accettazione, che si considera essenziale ai fini del pagamento dei corrispettivi dovuti secondo quanto previsto negli articoli 18, comma 6 e all'articolo 22, commi 11 e 12 del contratto esecutivo di ciascuno degli istituti aderenti.

In caso di esito negativo dei test, fatte salve le penali previste, il fornitore si impegna a svolgere ogni attività necessaria per risolvere i problemi evidenziati, restando a suo carico ogni onere derivante dalle attività suddette.
Il test non andato a buon fine potrà essere reiterato una sola volta con le medesime modalità e termini previsti, secondo quanto previsto dall'allegato 1 al presente capitolato e dal richiamato articolo 18 del contratto esecutivo di ciascuno degli istituti aderenti.

8 IL SERVIZIO DI AFFIANCAMENTO FINALE

Negli ultimi due mesi di validità del contratto, il Fornitore dovrà, su richiesta di ciascuno degli Istituti trasferire a personale degli stessi o a terzi da essi designati il know-how sulle attività condotte e tutta la documentazione tecnica ed operativa utile a consentire, in modo efficiente e senza interruzioni, l'eventuale prosecuzione delle attività da parte di un eventuale fornitore subentrante cui gli Istituti dovessero affidare le attività per assicurare il Disaster Recovery dei propri siti primari.
Possono essere previste attività di formazione, sessioni di lavoro congiunto, invio formale della documentazione relative alle soluzioni tecniche, alle configurazioni e alle procedure necessarie.
E' pertanto richiesto al Fornitore di predisporre un piano di lavoro di dettaglio delle attività di trasferimento di know how.
Le attività concordate e pianificate si considerano remunerate già nell'ambito del corrispettivo complessivo contrattuale; si rimanda all'articolo 16 del contratto esecutivo di ciascuno degli istituti aderenti.

9 INDICATORI DEI SERVIZI RICHIESTI PER LA SOLUZIONE DI DISASTER RECOVERY DEGLI ISTITUTI

Attraverso il Portale richiamato al precedente punto 4.1.2, il fornitore dovrà consentire al personale degli Istituti di verificare da remoto in qualsiasi momento lo stato delle attività, dei servizi svolti per assicurare la soluzione di Disaster Recovery e dei livelli di servizio riscontrati periodicamente nonché per monitorare lo stato delle risorse disponibili, dello storage esclusivo e delle connessioni trasmissive.
Ai fini del controllo della conformità ai livelli di servizio contrattuali di competenza di ogni singolo Istituto, nel Portale dovranno essere assicurate almeno le seguenti funzionalità:

- acquisizione dei dati di dettaglio necessari alla determinazione dei livelli di servizio;
- raccolta, aggregazione e normalizzazione dei dati di dettaglio, eventualmente provenienti da fonti diverse, ed elaborazione dei valori dei livelli di servizio con riferimento alla finestra temporale di osservazione prevista;
- produzione della rendicontazione dei livelli di servizio monitorati;
- memorizzazione affidabile e riservata dei dati archiviati, delle rendicontazione e dei deliverables che il Fornitore è tenuto a produrre per tutti i servizi;
- calcolo delle eventuali penali.

In allegato 1 al presente capitolato vengono riepilogati, sulla base di quanto prescritto dal presente Capitolato, i principali adempimenti e indicatori, le soglie previste e le penalità da applicare in caso di inadempienza per i servizi richiesti al fornitore, fermo restando, quanto previsto al successivo punto 14.2.

10 RENDICONTAZIONI, RIEPILOGO DEI DELIVERABLE DA PRODURRE E RENDERE ACCESSIBILI TRAMITE PORTALE; TERMINI DI APPROVAZIONE E/O RICHIESTA DI MODIFICA, INTEGRAZIONE, CORREZIONE DEI DELIVERABLE

Per ciascun Istituto, il Fornitore dovrà rendere disponibili ed accessibili via web, attraverso il Portale richiamato al precedente punto 4.1.2, i deliverable, i Piani e le rendicontazioni sui servizi resi e sui livelli di servizio, nonché le eventuali comunicazioni, segnalazioni e scambi di informazioni effettuate non direttamente attraverso il Portale bensì attraverso apposite comunicazioni formali, attraverso messaggi di PEC ovvero attraverso comunicazioni al numero verde.

A tal fine, il Portale messo a disposizione dal fornitore dovrà essere in grado di rilevare in modo il più possibile automatizzato tutti gli eventi rilevanti e consentire agli Istituti, per la parte di propria competenza, di verificare le attività svolte, i *deliverable* prodotti e di monitorare la conformità di quanto fornito agli indicatori e ai livelli di servizio previsti.
Il portale dovrà consentire in particolare, durante la fase di erogazione dei servizi, la rendicontazione giornaliera e settimanale dei valori di RPO osservati, fornendo a ciascun Istituto

report che riepiloghino in forma di grafico l'andamento delle attività di replica e copia dei dati, l'esito delle stesse e gli eventuali *alarm* in merito ad i casi in cui l'attività di replica ed allineamento dei dati fra i siti primari e il sito del NCUB non sia andata a buon fine o manifesti un superamento dei valori di RPO stabiliti nell'allegato 1.
Tutta la reportistica relativa dovra' essere archiviata e conservata a cura del Fornitore sul Portale per tutta la durata contrattuale.

In particolare, la rendicontazione sui servizi resi ed i livelli di servizio verrà presa come riferimento, in caso di inadempimento, per il calcolo delle penali.

Il fornitore, entro i 10 (dieci) giorni solari successivi al termine del mese di riferimento, dovrà produrre per ciascun Istituto apposita rendicontazione mensile sulle attività svolte per ciascuno dei servizi previsti, evidenziando, in modo puntuale, sempre per ciascuno degli Istituti:

- le attività svolte, i tempi di ripristino ed i livelli di servizio conseguiti nel mese;
- i giorni persona utilizzati per ciascuna delle risorse professionali previste e messe a disposizione per l'assistenza operativa ed il supporto al personale di ciascun Istituto;
- gli spazi attrezzati messi a disposizione per ospitare le configurazioni di emergenza;
- le risorse elaborative messe a disposizione (in termini di CPU per i server; in termini di Mips per le risorse operative in area Mainframe);
- le iniziative adottate per mantenere l'allineamento delle configurazioni di emergenza;
- le attività svolte per assicurare la manutenzione della soluzione di Disaster Recovery relativa a ciascun Istituto ed in particolare l'esito delle attività di test e verifica effettuate per assicurare il monitoraggio della soluzione di Disaster Recovery;
- gli eventuali interventi effettuati e le eventuali variazioni apportate in forza dei punti 9 e 10;
- le eventuali criticità che si ritiene debbano essere risolte, unitamente alle proposte che il fornitore intenderebbe adottare, con precisazioni in merito ai relativi termini e modalità di realizzazione degli interventi di miglioramento/soluzione proposti

Come si è già avuto modo di evidenziare, nel corso del periodo di erogazione dei servizi, il Fornitore dovrà predisporre e sottoporre all'approvazione di ciascuno degli Istituti attraverso il Portale ovvero con le modalità di comunicazione e tracciatura definite nel Piano di Progetto i deliverable e documenti di seguito sinteticamente richiamati.
Ciascun Istituto si riserva la facoltà di chiedere il supporto e la supervisione della segreteria tecnica di DigitPA nelle fasi di verifica ed approvazione delle rendicontazioni e dei *deliverable* previsti, secondo quanto previsto nell'articolo 6 del contratto quadro.
Si riporta una sintesi dei relativi termini di consegna e di approvazione, nonchè dei termini per la eventuale emissione della nuova versione del deliverable in caso di richiesta di modifica, integrazione e correzione.
Si rimanda a quanto riportato nel contratto e nell'allegato 1 al presente Capitolato per i casi di inadempienza o ritardo nella consegna:

Deliverable previsto	**Termine di consegna/disponibilità sul Portale**	**Termine di approvazione/accettazione o per la richiesta di modifiche, integrazioni e correzioni**	**Termini per la eventuale emissione ed approvazione della nuova versione del deliverable in caso di richiesta di modifica, integrazione e correzione**
Piano di progetto generale e Piano della Qualità della Fornitura	Entro i primi 60 (sessanta) giorni solari dalla sottoscrizione del contratto quadro per il primo anno di vigenza contrattuale (per il Piano di progetto generale iniziale) e entro i 30 (trenta) giorni solari precedenti all'inizio di ciascun anno per i	Entro i 30 (trenta) giorni solari successivi alla ricezione del piano annuale.	Entro i 15 (quindici) giorni solari dalla data di ricezione della richiesta di modifica, integrazione o correzione sottoponendo all'Istituto una nuova versione del Piano. Per l'approvazione della nuova versione del piano, oggetto di rilievo o richiesta di modifica,

	successivi anni di vigenza del contratto (per il Piano di progetto generale annuale) Il Piano di Progetto Generale potrà essere sottoposto a revisione anche a fronte di rilevanti variazioni tecnico organizzative, e dovrà, quindi, essere sottoposto all'approvazione dell'Istituto/degli Istituti interessati, entro i 30 (trenta) giorni solari successivi alla richiesta di revisione, formalizzata dall'Istituto/dagli Istituti interessati.		integrazione e correzione sono da intendersi fermi sempre i 15 (quindici) giorni solari successivi alla data di ricezione del piano stesso.
Rendicontazione settimanale dei livelli RPO giornalieri di tutta la settimana	Entro il primo giorno della settimana successiva a quella di rilevazione	Entro i 5 giorni solari successivi alla consegna o alla messa a disposizione dei report sul Portale	
Rendicontazione mensile sui servizi resi ed i livelli di servizio	Entro i 10 (dieci) giorni solari successivi al termine del mese di riferimento, per ciascun Istituto aderente al Centro	Entro i 10 (dieci) giorni solari successivi alla data di ricezione della rendicontazione mensile	Entro i 10 (dieci) giorni solari successivi alla data di ricezione della richiesta di modifica, integrazione e correzione
Piano di Disaster Recovery	Entro i primi cinque mesi di vigenza del contratto per il primo anno di erogazione dei servizi e, entro i 30 (trenta) giorni solari precedenti all'inizio di ciascun anno per i successivi anni di vigenza del contratto. Il Piano di Disaster Recovery potrà essere sottoposto a revisione anche a fronte di rilevanti variazioni tecnico organizzative, e sottoposto all'approvazione dell'Istituto/degli Istituti interessati, entro i 30 (trenta) giorni solari successivi alla richiesta di revisione, formalizzata dall'Istituto/dagli Istituti interessati. Il Piano di DR potrà essere sottoposto a verifica ed eventuale revisione anche con cadenza semestrale secondo quanto previsto al punto 7 del Capitolato	Entro i 15 (quindici) giorni solari successivi alla data di ricezione	Entro i 15 (quindici) giorni solari dalla data di ricezione della richiesta di modifica, integrazione o correzione sottoponendo all'Istituto una nuova versione del Piano. Per l'approvazione della nuova versione del piano, oggetto di rilievo o richiesta di modifica, integrazione e correzione sono da intendersi fermi sempre i 15 (quindici) giorni solari successivi alla data di ricezione del piano stesso.

	tecnico		
Documentazione delle procedure operative e dei criteri di esecuzione dei test periodici	Entro i primi cinque mesi di vigenza del contratto per il primo anno di erogazione dei servizi e, entro i 30 (trenta) giorni solari precedenti all'inizio di ciascun anno per i successivi anni di vigenza del contratto	Entro il termine di 15 (quindici) giorni solari successivi alla data di ricezione	Entro i 15 (quindici) giorni solari successivi alla data di ricezione della richiesta di modifica, integrazione e correzione Per l'approvazione delle nuove versioni della documentazione a seguito di rilievo o richiesta di modifica, integrazione e correzione sono da intendersi fermi sempre i 15 (quindici) giorni solari successivi alla data di ricezione del piano stesso
Stato avanzamento lavori (Verifiche semestrali)	Entro i 30 (trenta) giorni solari successivi alla fine del semestre di riferimento	Entro i 30 (trenta) giorni solari successivi alla data di ricezione	Entro i 15 (quindici) giorni solari dalla data di ricezione della richiesta di modifica, integrazione o correzione sottoponendo all'Istituto una nuova versione del Piano.
Esiti dei test periodici previsti (ogni semestre)	La data per l'effettuazione dei test è da definire dalle parti con preavviso di trenta giorni, unitamente alle attività da svolgere e al termini di completamento dei test e di consegna dei relativi esisti	Entro il termine di 10 (dieci) giorni solari successivi alla data di ricezione	Entro i 15 (quindici) giorni solari successivi alla data di ricezione della richiesta di modifica, integrazione e correzione
Piano di lavoro di dettaglio delle attività di affiancamento finale e trasferimento di know how.	Entro i 10 giorni solari successivi alla richiesta	Entro i 10 (dieci) giorni solari successivi alla ricezione dello stesso.	Entro i **10 (dieci)** giorni solari successivi alla data di ricezione della richiesta di modifica, integrazione e correzione.

Per tutti i deliverable previsti, entro i relativi termini previsti e richiamati nella precedente tabella ed in particolare negli articoli 7, 8, 14, 15, 16 del contratto esecutivo di ciascuno degli istituti aderenti, ciascun Istituto si riserva, attraverso il Portale ovvero con le modalità di comunicazione e tracciatura definite nel Piano di Progetto di chiedere modifiche, integrazioni o correzioni e il Fornitore stesso è obbligato a recepire le modifiche, integrazioni e correzioni richieste, sottoponendo all'approvazione dell'Istituto interessato una nuova versione del deliverable non accettato, entro termini richiamati sempre nel contratto e nella precedente tabella, che decorrono dalla data di ricezione della richiesta di modifica, integrazione e correzione, comunque formalizzata.

L'Istituto, verificato che le modifiche, integrazioni o correzioni richieste siano state apportate, attraverso il Portale ovvero con le modalità di comunicazione e tracciatura definite nel Piano di Progetto, si riserva di approvare la nuova versione del deliverable oggetto di rilievo entro i termini previsti e richiamati nel contratto e nella precedente tabella, che decorrono dalla data di ricezione della stessa.

Il Fornitore si impegna comunque, nel periodo necessario alla definizione ed approvazione dei deliverable, a svolgere le attività previste senza interruzioni e disagi per gli Istituti e per l'utenza.

11 VERIFICA DELLA QUALITA' DEI SERVIZI

Il Piano della Qualità dei servizi dovrà contenere la descrizione degli obiettivi di qualità dei servizi oggetto della fornitura, delle risorse e delle tecniche, metodologie e strumenti che il fornitore adotterà per assicurare la qualità della fornitura, secondo i contenuti di massima delineati nell'allegato relativo.
Il Piano della Qualità costituirà il riferimento per le attività di verifica e validazione svolte dal Fornitore e dovrà essere prodotto nei tempi previsti dai precedenti punti 4 e 10.
Ogni modifica al Piano della Qualità dovrà essere sottoposta ad approvazione secondo quanto previsto nel precedente punto 10.
Ogni strumento ed accorgimento adottato per l'effettuazione e la rilevazione delle misure necessarie a valutare il rispetto dei requisiti di qualità e dei livelli di servizio durante il periodo di validità del contratto sarà a carico del fornitore.
A carico del fornitore è anche la elaborazione, conservazione e presentazione delle misure, nelle modalità e nei formati previsti.
Ciascun Istituto si riserva di verificare la correttezza dei metodi di rilevazione adottati e la correttezza delle misure rilevate, anche a campione.
La valutazione del rispetto dei requisiti di qualità oltreche dei livelli di servizio è come evidenziato nel presente Capitolato effettuata dagli Istituti aderenti, avvalendosi a tal fine di tutte le misure e rendicontazioni rese disponibili dal fornitore. Gli Istituti aderenti si riservano comunque la facoltà di affidare tale incarico di valutazione e verifica anche ad esperti esterni e di attivare un monitoraggio della fornitura secondo i presupposti e le disposizioni della normativa vigente in materia.

12 CRITERI DI VALORIZZAZIONE E VARIAZIONE DEI SERVIZI

Il Fornitore si impegna ad eseguire i servizi previsti secondo quanto definito nel contratto quadro, nei contratti esecutivi, nel Capitolato e nei suoi allegati, senza avere diritto ad alcun compenso ulteriore, oltre il corrispettivo previsto, che costituisce il massimale economico cui gli Istituti aderenti, ciascuno per la parte di propria competenza, hanno facoltà di attingere sulla base delle necessità connesse all'attuazione del progetto.
Le parti si danno che atto a partire dal secondo anno di vigenza contrattuale, le somme stanziate da ciascun Istituto per la soluzione di Disaster Recovery richiesta tengono conto anche della facoltà di incremento o diminuzione regolata nei contratti esecutivi di ciascuno degli Istituti aderenti.
Il fornitore si impegna in occasione della pianificazione annuale nonché ove necessario in occasione delle verifiche semestrali di cui al successivo punto 13 e secondo quanto previsto dal contratto esecutivo di ciascuno degli Istituti aderenti, a mantenere aggiornati e se necessario, evolvere gli ambiti e i servizi coperti dalla soluzione di DR.
Il Fornitore, ai fini della pianificazione a preventivo, si impegna anche a proporre nel piano annuale, sulla base dei consuntivi dell'anno precedente, come rimodulare nell'ambito del corrispettivo annuo complessivo i corrispettivi dei vari servizi per tener conto delle eventuali evoluzioni dell'architettura e delle configurazioni esistenti, adottate su richiesta dell'Istituto interessato, per tener conto di eventuali mutamenti alle esigenze operative e del contesto tecnologico che abbiano reso necessario ridefinire/ampliare i processi, le applicazioni e i relativi dati per i quali deve essere adottata la soluzione di Disaster Recovery.
Si rimanda a quanto previsto negli articoli 22, 23 e 25 del contratto.

13 VERIFICHE SEMESTRALI DEI SERVIZI DI DISASTER RECOVERY

Il fornitore si impegna entro i primi 30 giorni solari successivi alla fine di ciascun semestre a predisporre e sottoporre all'accettazione/approvazione di ciascuno degli Istituti aderenti, un documento denominato "stato avanzamento lavori semestrale" che consentirà la verifica dell'adeguatezza della soluzione e del relativo piano di Disaster Recovery nonché la periodica revisione delle configurazioni.
In occasione delle verifiche semestrali il fornitore si impegna a fornire:

- indicazioni del consuntivo complessivo delle attività svolte nel semestre precedente;

- evidenza:
  – delle eventuali criticità riscontrate nel semestre, nel corso dell'erogazione dei servizi e/o dei test periodici;
  – delle eventuali evoluzioni da apportare su richiesta degli Istituti, all'architettura, alle configurazioni esistenti ed alla soluzione di Disaster Recovery, che si rendano necessari per tener conto di mutamenti o variazioni delle esigenze operative e del contesto tecnico di riferimento degli Istituti;
  – delle eventuali evoluzioni, da apportare su richiesta degli Istituti;
  – dell'eventuale necessità di rimodulare i corrispettivi dovuti per i servizi compresi nella soluzione di DR, fermo l'importo complessivo annuo definito per assicurare a ciascun Istituto i servizi compresi nella soluzione di DR.

Ciascun Istituto aderente si riserva ove necessario di avvalersi del supporto e della supervisione di DigitPA, attraverso la segreteria tecnica (secondo quanto previsto nell'articolo 6 e nell'articolo 12 del contratto quadro); a tal fine l'Istituto è tenuto a inviare apposita comunicazione alla segreteria tecnica di DigitPA.
Ciascun istituto si riserva di chiedere modifiche, integrazioni o correzioni, sia di tener conto delle previsioni formulate, sia di definire, nell'ambito degli importi massimali allo stesso assegnati, come eventualmente rimodulare le spese previste e dettagliate nel rispettivo contratto esecutivo.
Si rimanda a quanto previsto dagli articoli 15, 22 e 23 del richiamato contratto esecutivo di ciascuno degli Istituti aderenti.

14 VARIAZIONI IN CORSO D'OPERA

14.1 Variazioni in corso d'opera

A partire dal secondo anno di vigenza contrattuale, secondo quanto previsto nell'articolo 22 del contratto esecutivo di ciascuno degli istituti aderenti, ciascun Istituto si riserva la facoltà, tenuto conto del massimale economico annuo di base definito, di avvalersi della possibilità di incremento o diminuzione entro un massimale del 5% dell'importo annuo di base relativo al complesso dei servizi erogati dal Fornitore per la soluzione di Disaster Recovery prevista per rimodulare, ove necessario, i canoni mensili previsti.

14.2 Variazioni e/o revisioni dei livelli di servizio (con eventuale adeguamento – incremento o riduzione - dei corrispettivi mensili)

Ciascun Istituto si riserva la facoltà di richiedere, attraverso apposita comunicazione scritta, che siano definite, a seguito di apposito incontro definito di riesame, delle variazioni e/o revisioni dei livelli di servizio, secondo quanto previsto dall'articolo 23 del contratto esecutivo di ciascuno degli istituti aderenti.

A partire dal mese successivo a quello nel quale si sarà svolto e concluso con apposito verbale l'incontro di riesame per definire le variazioni e/o revisioni dei livelli di servizio, il fornitore dovrà provvedere a fatturare i corrispettivi previsti con adeguamento in aumento o diminuzione del relativo importo mensile.

15 ADEGUAMENTO DEI CORRISPETTIVI A SEGUITO DELL'ESERCIZIO DELLA FACOLTA' DI RICORRERE AL QUINTO D'OBBLIGO

Gli Istituti si riservano la facoltà di ricorrere al quinto d'obbligo, ai sensi dell'articolo 11 del R.D. 18 novembre 1923, n. 2440.

In caso di esercizio della facoltà di cui trattasi in aumento o in diminuzione le attività e i termini relativi alle prestazioni che devono essere incrementate o diminuite (nonché le eventuali modifiche e aggiornamenti che devono essere apportate alla configurazione d'emergenza e alla soluzione di Disaster Recovery), saranno definiti in apposito piano di dettaglio per l'adeguamento a fronte del quinto d'obbligo, secondo quanto previsto nell'articolo 25 del contratto esecutivo di ciascuno degli

Istituti aderenti.

Le eventuali prestazioni integrative richieste verranno eseguite alle condizioni stabilite nel contratto quadro, nei contratti esecutivi degli istituti, nel presente capitolato e nei relativi allegati.

In caso di esercizio della facoltà di ricorso al quinto d'obbligo nel piano verrà data indicazione della quota che dovrà andare ad incrementare o della quota che andrà detratta dai corrispettivi dovuti al fornitore a seguito delle prestazioni che vengono richieste in aggiunta o in diminuzione a seguito del ricorso al qauinto d'obbligo.

16 ELENCO DI MASSIMA E VALORE DEGLI ALLEGATI

Si considerano parte integrante degli obblighi assunti dal fornitore quanto previsto negli allegati al presente Capitolato di seguito richiamati:

- Allegato 1: Descrizione dei principali adempimenti e indicatori, delle soglie previste e delle penalità da applicare in caso di inadempienza per i servizi richiesti al fornitore;
- Allegato 2: Descrizione delle postazioni di lavoro da garantire presso il NCUB;
- Allegato 3: Descrizione del contesto tecnologico dell'INPS e della soluzione di Disaster Recovery richiesta;
- Allegato 4: Descrizione del contesto tecnologico dell'INPS – ex IPOST e della soluzione di Disaster Recovery richiesta
- Allegato 5: Descrizione del contesto tecnologico dell'INAIL e della soluzione di Disaster Recovery richiesta;
- Allegato 6: Descrizione del contesto tecnologico dell'INPDAP e della soluzione di Disaster Recovery richiesta;
- Allegato 7: Descrizione di massima dei contenuti del Piano di Disaster Recovery;
- Allegato 8: Descrizione di massima dei contenuti del Piano di Progetto e del Piano di Qualità.
- Allegato 9: Descrizione della componente TLC necessaria alla soluzione di Disaster Recovery.