**BOZZA PRELIMINARE**

## ALLEGATO 4

# DESCRIZIONE DEL CONTESTO TECNOLOGICO DELL'IPOST E DELLA SOLUZIONE DI DISASTER RECOVERY RICHIESTA

# BOZZA PRELIMINARE

INDICE

# BOZZA PRELIMINARE

## 1. PREMESSA

Il documento fornisce la descrizione dei requisiti che dovranno essere rispettati nell'ambito della nuova gara in collaborazione con Digit PA, relativamente al Centro Unico di Backup per il Disaster Recovery geografico dell'infrastruttura IT dell'Istituto.

Il documento è articolato nei seguenti punti:

- Contesto di riferimento:
  - L'infrastruttura del sito primario IPOST di viale Asia
  - L'attuale soluzione di rete
  - Gli attuali livelli di servizio
- Soluzione di continuità operativa :
  - Aspetti tecnologici
  - Aspetti procedurali

### 1.1 SCOPO DEL DOCUMENTO

Scopo del presente documento è quello di descrivere i requisiti della soluzione di Disaster Recovery oggetto della gara in via di definizione in collaborazione con Digit PA e gli altri Enti previdenziali.

### 1.2 ABBREVIAZIONI

IPOST = Istituto Previdenza dei Postelegrafonici

S.I. IPOST = Sistema Informativo IPOST

## 2. DESCRIZIONE DEL CONTESTO TECNOLOGICO DI RIFERIMENTO

La strategia di Disaster Recovery adottata dall'Istituto prevede di far fronte ad eventi, disastrosi e non, facendo ripartire il sistema informatico dell'Istituto su un sito alternativo a partire da applicazioni e dati, siano essi su disco o su nastro, dei quali viene fatta una copia remota, pressoché istantanea e logicamente consistente, grazie ad un meccanismo di mirroring che non genera impatti, in termini di tempi di risposta, sulle applicazioni di esercizio.

Il termine identifica l'insieme delle misure necessarie a garantire la continuità operativa e il ripristino del Sistema Informatico a seguito dell'indisponibilità accidentale di un centro di elaborazione dati o di una sua parte vitale.

La strategia alla base della **Disaster Recovery** prevede che le attività di elaborazione e di comunicazione vengano ripristinate attivando un sito alternativo geograficamente distante da quello che si è reso non disponibile. A causa delle condizioni in cui si deve operare in caso di disastro, è evidente che la mera disponibilità delle risorse alternative e dei dati non sono di per sé sufficienti a garantire il successo dell'intera operazione di ripristino.

Da queste considerazioni scaturisce l'esigenza di predisporre un **Piano di Disaster Recovery o Contingency Plan,** che descriva l'insieme omogeneo e coordinato di azioni da intraprendere prima, durante e dopo il verificarsi di un disastro; nasce inoltre la necessità di controllare, periodicamente e indipendentemente dall'evento disastroso, la validità delle misure previste dal Piano.

Infatti, solo la preventiva definizione dell'organizzazione necessaria, in termini di compiti, ruoli, responsabilità, figure professionali, dei passi procedurali, delle attività e della loro schedulazione, insieme al collaudo periodico del corretto funzionamento delle diverse componenti in gioco e dell'integrazione delle varie persone coinvolte, sono la garanzia di successo nella gestione di un eventuale disastro.

Le isole applicative coperte dalla soluzione di BC/DR saranno le seguenti:

- **SAP R/3 (Sol Manager, Sviluppo, Test e Produzione)**
- **SAP BW (Sviluppo, Quality e Produzione)**
- **NAI**
- **Teleforum**
- **Domain Controller**
- **Server di backup**

# BOZZA PRELIMINARE

## 3. ORGANIZZAZIONE E PROCEDURE PER LA GESTIONE DELLA CONTINUITà OPERATIVA

PIANO DI DISASTER RECOVERY

L'adozione dell'attuale soluzione di Business Continuity/Disaster Recovery (BC/DR) ha comportato non solo la revisione/adeguamento dell'infrastruttura di produzione e delle procedure di recovery, ma ha portato anche alla definizione delle procedure e strutture organizzative deputate a presiedere il governo delle crisi informatiche.

L'attuale organizzazione di gestione delle crisi prevede procedure tecnico-organizzative da seguire per attivare le configurazioni di emergenza, così come i ruoli e le responsabilità sia del personale dell'Istituto che di quello dei Fornitori, regolamentate con una serie di norme contenute nel Piano di ripristino. Per l'approntamento e l'attuazione di tali norme, l'Istituto ha coinvolto le funzioni aziendali interne ed esterne ritenute necessarie per la gestione dell'emergenza informatica, per la gestione del personale, nonché per le comunicazioni esterne, ecc...

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

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

- Rilevare lo stato di emergenza;
- Dare il preallarme;
- Attivare formalmente ed operativamente il Piano di ripristino;
- Gestire il rientro al termine dello stato di crisi.

Nell'ambito dell'iniziativa del Centro Unico di Backup, a cui aderiscono oltre ad IPOST anche INPS, INAIL e INPDAP, nel caso in cui l'IPOST dichiari lo stato di emergenza, il Comitato di Crisi comunicherà all'omologo Comitato di ciascuno degli altri Istituti ed alla Segreteria Tecnica del CUB, coordinata da Digit PA, la situazione e la stima del tempo di permanenza presso la struttura di recovery.

Il Comitato di Crisi si avvale del Comitato di Coordinamento Tecnico per valutare entità e durata della condizione di emergenza e per adottare le opportune azioni secondo quanto previsto nel Piano di recovery.

# BOZZA PRELIMINARE

## 4. CONFIGURAZIONE DI RIFERIMENTO IT

### 4.1 INFRASTRUTTURA REPLICABILE PRESSO IL CUB

#### 4.1.1. INFRASTRUTTURA TECNICA DA REPLICARE PRESSO IL CUB

| Q.tà | Configurazione |
|---|---|
| 1 | **IBM xSeries X3650 (Teleforum)**<br>2 x Xeon Quad-Core X5365 3.0GHz<br>6 GB RAM<br>2 x 73 GB internal SAS HDD<br>4 x 146 GB internal SAS HDD<br>2 x Ethernet adapters<br>xSeries 835W Redundant Power Option |
| 1 | **IBM xSeries X3850 (Teleforum)**<br>4 x Intel Xeon Dual Core Processor Model 7130N 3.16GHz<br>8 GB RAM<br>4 x IBM 146GB 2.5in 10K HS SAS HDD<br>1 x ServeRAID 8i SAS Controller<br>2 x Ethernet adapters<br>1300 Watt Power Supply Option |
| 2 | **IBM xSeries X366 (SAP)**<br>4 x XEON 3.16Ghz<br>4 GB ram<br>2 x 36 GB disco interno |
| 2 | **IBM xSeries X346 (Protocollo)**<br>1 x XEON 2.8 Ghz<br>2 GB ram<br>2 x 36 GB disco interno |
| 1 | **IBM xSeries X346 (Portale)**<br>1 x XEON 2.8 Ghz<br>2 GB ram<br>2 x 36 GB disco interno |
| 1 | **IBM xSeries X346 (Posta Elettronica)**<br>1 x XEON 2.8 Ghz<br>2 GB ram<br>2 x 36 GB disco interno |
| 2 | **IBM xSeries X346 (Domain Controller, DNS, DHCP, WAC)**<br>1 x XEON 2.8 Ghz<br>2 GB ram<br>2 x 36 GB disco interno |
| 1 | **IBM xSeries X346 (Firewall 1)**<br>1 x XEON 2.8 Ghz<br>2 GB ram<br>2 x 36 GB disco interno<br>3 adattatori di rete |

| | |
|---|---|
| 1 | **IBM xSeries X346 (Portale Intranet)**<br>1 x XEON 2.8 Ghz<br>2 GB ram<br>2 x 36 GB disco interno |
| 2 | **IBM xSeries X346 (Fax Server)**<br>1 x XEON 3.0 Ghz<br>1 GB ram<br>2 x 146 GB disco interno |
| 1 | **IBM xSeries X346 (Firewall 2)**<br>2 x XEON 2.8 Ghz<br>2 GB ram<br>2 x 36 GB disco interno<br>3 adattatori di rete |
| 1 | **IBM xSeries X346 (Server FTP)**<br>1 x XEON 3.4 Ghz<br>2 GB ram<br>2 x 36 GB disco interno |
| 1 | **IBM xSeries X236 (Mandante SAP)**<br>2 x XEON 3.0 Ghz<br>4 GB ram<br>2 x 36 + 5 x 73 GB disco interno |

***Tabella 1 – Configurazione dei server presso il CUB***

Tutti i server xSeries sopraelencati dispongono di unità a nastro DAT in formato DDS5/DAT72, retrocompatibile con DDS4 e DDS3. Sono, inoltre, presenti nr. 2 unità a nastro di tipo LTO

| Q.tà | Configurazione |
|---|---|
| 4 | **Workstation IBM ThinkCentre A Series**<br>1 CPU 2.4 Ghz<br>256 MB RAM<br>40 GB disco interno |

***Tabella 2 – Configurazione delle workstation presso il CUB***

| Q.tà | Configurazione |
|---|---|
| 1 | **Cisco Catalyst 3750** 24 10/100/1000T Standard Multilayer Image<br>WS-C3750G-24T-S |
| 1 | **Cisco StackWise 50CM** Stacking Cable<br>CAB-STACK-50CM |
| 1 | **Power Cord-Italian**<br>CAB-ACI |
| 2 | **GE SFP, LC connector SX transceiver**<br>GLC-SX-MM= |

***Tabella 3 – Configurazione dispositivi di rete presso il CUB***

Le risorse elaborative coinvolte nel progetto includono anche un server IBM pSeries mod. 55A ed il relativo sottosistema storage IBM TotalStorage DS4700, di proprietà dell'Istituto e già installati presso il CUB, con le seguenti caratteristiche:

| Q.tà | Configurazione |
|---|---|
| 1 | **IBM pSeries 9133-55A**<br>2 x 1,65Ghz Power5+<br>10 GB RAM<br>2 x 73 GB internal HDD<br>2 x Fibre Channel adapters<br>2 x Ethernet adapters<br>1 x 4mm internal tape drive |
| 1 | **IBM TotalStorage DS4700**<br>2 x Fibre Channel adapters<br>14 x 146,8 GB / 10K rpm disk drives |

***Tabella 4 – Configurazione server pSeries e relativo storage c/o CUB***

## 4.2 DESCRIZIONE ATTUALI LIVELLI DI SERVIZIO PRESSO IL CUB

La soluzione di Disaster Recovery attualmente implementata per IPOST vede la sua funzionalità principale nella realizzazione di una copia consistente (su nastro) dei dati dei sistemi coperti dal servizio di BC/DR.

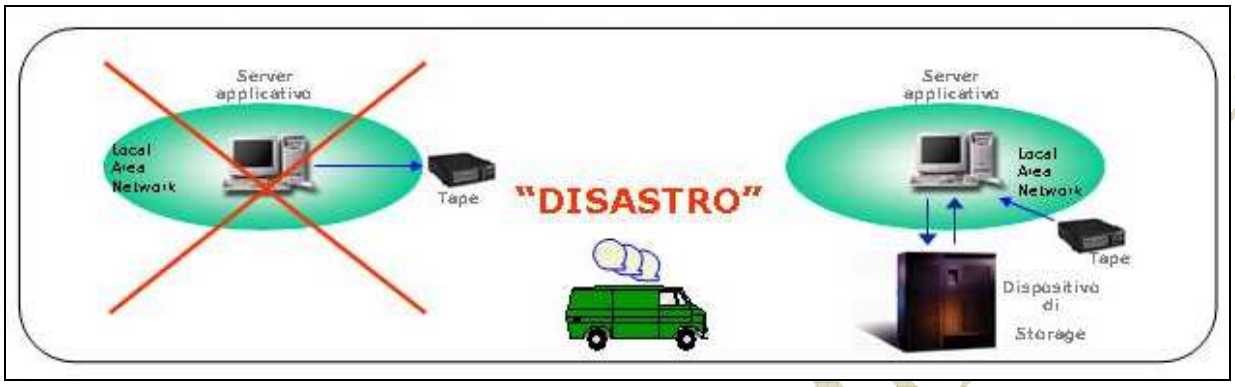



*Figura 1 – Architettura della soluzione*

In condizioni di operatività normale i dati del centro primario vengono salvati su nastro adottando opportune politiche di salvataggio determinate dalla criticità dei servizi erogati e dei dati da salvaguardare.

In tali condizioni nel centro di backup non è richiesta la presenza di macchinari attivi. I server applicativi, destinati ad essere utilizzati in caso di indisponibilità del centro primario, pur essendo fisicamente presenti, non hanno la necessità di rimanere accesi.

I nastri contenenti i dati salvati saranno trasportati settimanalmente presso un caveau di massima sicurezza e resi disponibili in caso di necessità.

In condizioni di disastro, i server presenti nel centro di backup saranno accesi, e, opportunamente configurati, caricheranno da nastro l'ultima copia di dati salvati nel sito primario.

### 4.2.1. RTO E RPO ATTUALI

Associati alle due diverse soluzioni di allineamento dati sul sito di Disaster Recovery ci sono i Livelli di Servizio di seguito riassunti:

| | RTO | RPO | **Stato dei servizi** |
|---|---|---|---|
| Configurazione di emergenza | = 72 ore | □ 7 gg. | I servizi di infrastruttura presso il CUB sono: tape drive, sistemi oggetto di ripristino a freddo |

**Tabella 1 – Livelli di servizio soluzione a freddo**

Per la soluzione a freddo, il valore di RPO è rappresentato dal momento di esecuzione dell'ultimo salvataggio completato con successo e trasportato presso il CUB.

### 4.2.2. LA SOLUZIONE PROGETTUALE DI TRASPORTO

La soluzione progettuale di trasporto della soluzione di Disaster Recovery è stata sviluppata per consentire il soddisfacimento dei seguenti requisiti:

- consentire il Disaster Recovery delle applicazioni istituzionali secondo i vincoli sistemistici;
- prevedere sul CED di backup un'infrastruttura di sicurezza con architettura analoga a quella già presente nel CED primario, in grado di garantire le necessarie politiche di sicurezza sia nei casi di failure del sito principale che durante l'esercizio contemporaneo dei due siti.

# BOZZA PRELIMINARE

## 5. SOLUZIONE DI DISASTER RECOVERY RICHIESTA

RIPRENDERE LE CONFIGURAZIONI ATTUALI E PER SINGOLA MACCHINA O GRUPPO DI QUESTE METTERE TUTTE LE INDICAZIONI PUNTUALI… ETC
DETTAGLIO DELLO STORAGE RICHIESTO…CON LIVELLO DI DETTAGLIO MINIMO

### 5.1 ASPETTI TECNOLOGICI

La fornitura di spazi, infrastruttura logistica, servizi, sistemi ed apparati consentiranno la realizzazione di una soluzione di Disaster Recovery che consenta all'Istituto, in caso di cessazione totale o parziale della operatività del suo Sistema di Elaborazione Dati, la ripartenza presso il sito secondario o di recovery.

Relativamente all'infrastruttura descritta nei paragrafi precedenti, di seguito si riportano le esigenze di protezione dal disastro.

**Servizi IT**

La soluzione richiesta per il Disaster Recovery presso il centro unico di backup (CUB Geografico) dovrà prevedere la disponibilità per l'Istituto di tutti i servizi erogati presso il Ced principale dell'Ipost da sistemi ed apparati descritti nei paragrafi precedenti e negli allegati.

L'allineamento dell'ambiente secondario (di Disaster Recovery) rispetto al Sito Principale avverrà secondo la tipologia di copia dei dati "**a freddo**" (backup in asincrono ed allineamento differito con il centro di backup) per tutte le piattaforme di Esercizio.

### 5.2 ASPETTI PROCEDURALI

La tipologia del servizio offerto dal Fornitore e i ruoli ricoperti da Fornitore ed Istituto rispecchieranno praticamente quelli del contratto attualmente in essere.

Il Fornitore sarà responsabile:

- della predisposizione e della funzionalità della infrastruttura hw, sw di sistema, di rete. Non è esplicitamente richiesto che le risorse hw siano "dedicate" e quindi non sarà potrebbe non essere possibile richiedere la disponibilità continua delle risorse "sistemi". Il Fornitore sarà tuttavia tenuto a garantire, in fase di test o di dichiarazione di disastro, la disponibilità delle percentuali di capacità elaborativa previste contrattualmente, da dimostrare attraverso opportuni appositi report. Per quanto riguarda invece lo spazio disco, questo sarà di esclusiva pertinenza dell'Istituto che potrà monitorare da remoto o tramite la verifica di archivi, log di sistema, ecc. l'effettiva presenza dei requisiti previsti (in termini di spazio a disposizione e di tipologia dello storage predisposto).

- Dell'allineamento delle configurazioni hw, una volta che l'Istituto abbia comunicato eventuali variazioni che rientrino nel "perimetro" di quelle applicabili in base al contratto;
- Della disponibilità dei sistemi entro i tempi previsti da contratto, sia per le fasi di test che in caso di dichiarazione di disastro. In tali occasioni i sistemi andranno "rilasciati" ai sistemisti dell'Istituto accessi e con il sw di sistema correttamente lanciato ed in esecuzione. Sarà cura dell'Istituto avviare sw di ambiente, databases, applicazioni.
- Della produzione della documentazione prevista contrattualmente

L'Istituto sarà responsabile:

- Della comunicazione delle configurazioni dei sistemi.
- Della comunicazione della corretta sequenza di accensione dei sistemi.
- Della tempestiva e puntuale notifica al Fornitore di ogni modifica alla configurazione hw e/o di rete avvenuta presso il Ced di Esercizio;
- Del corretto avvio di sw di ambiente, DB e applicazioni.

In caso di test pianificato o di dichiarazione di disastro, l'Istituto attiverà, secondo le modalità previste dai documenti contrattuali, il Fornitore il quale effettuerà l'accensione dei sistemi e delle apparecchiature secondo quanto preventivamente comunicato dall'Istituto.

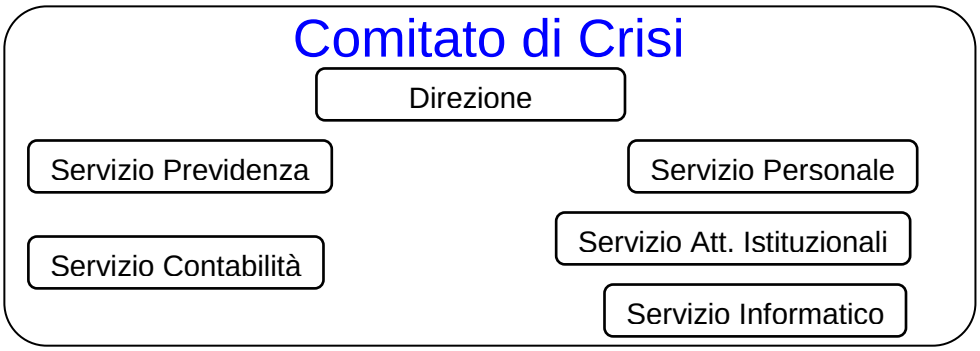
Una volta effettuata l'accensione fisica dei sistemi, il Fornitore provvederà al loro bootstrap (avvio dei vari sistemi operativi), verificando che questo avvenga in maniera corretta e completa, rilasciando quindi all'Istituto i sistemi in una situazione "pulita" e consistente, adatta all'avvio, da parte dei sistemisti Ipost, del sw di ambiente, dei databases e delle applicazioni.

In caso di problemi in fase di avvio, i sistemisti del Fornitore e dell'Istituto collaboreranno al fine di individuare, congiuntamente, quale sia la causa del mancato corretto avvio dell'ambiente, al fine di rimuovere prontamente il malfunzionamento verificatosi.

### 5.3 ASPETTI PROCEDURALI

Di seguito viene brevemente descritta l'organizzazione dell'Ipost atta a gestire e coordinare un eventuale caso di disastro:

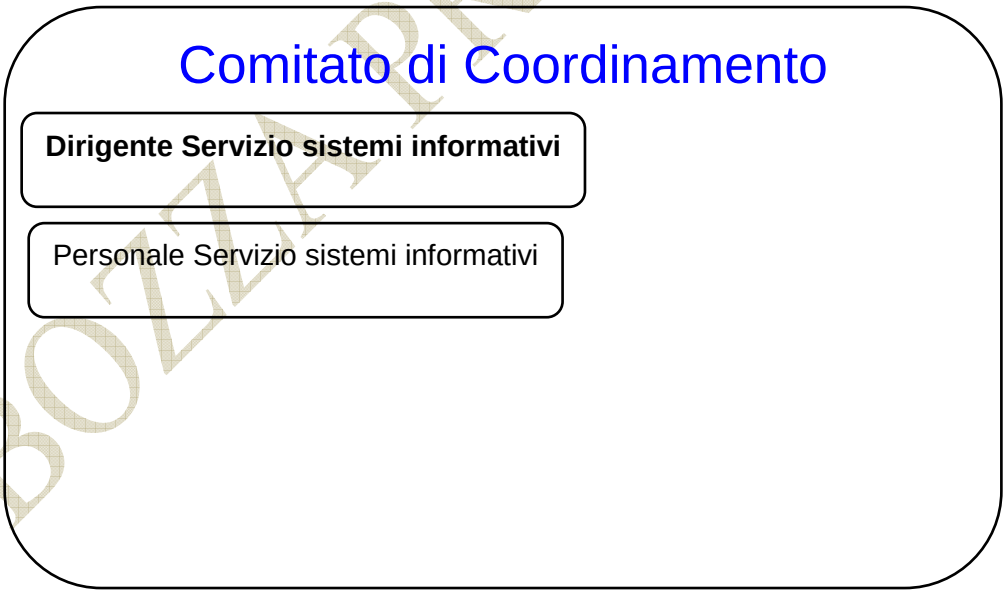
- **Comitato di Crisi**, così composto




Le responsabilità del Comitato di Crisi sono:

- Conoscere l'intero processo di recovery e il Piano di DR
- Formalizzare politiche e responsabilità
- Dichiarare lo Stato di Crisi
- Notificare il Disastro al Sito Alternativo
- Comunicare il Disastro agli Enti Esterni ed alla Segreteria del CUB
- Individuare il sito/sede di rientro
- Mettere a punto il piano di rientro
- Comunicare la fine dello Stato di Emergenza

- **Comitato di Coordinamento**, così composto




Le responsabilità del Comitato di Coordinamento sono:

- Conoscere l'intero processo di recovery e il Piano di DR

- Formalizzare procedure e responsabilità
- Gestire operativamente il Piano di DR (prove, revisioni)
- Valutare il potenziale disastro
- Supportare il Comitato di crisi
- Dare il preallarme
- Attivare la squadra di intervento
- Comunicare il disastro ai fornitori sw e alla periferia
- Comunicare al personale lo spostamento presso le sedi alternative
- Attivare operativamente il piano
- Gestire il rientro

- **Squadra d'Intervento**

La Squadra di Intervento, che costituisce il livello operativo della struttura permanente di Disaster Recovery è costituita dal personale tecnico-operativo addetto ai sistemi.

Le responsabilità della Squadra d'Intervento sono:

- Conoscere l'intero processo di recovery e il Piano di DR
- Mantenere le procedure operative
- Eseguire le prove del Piano di DR
- Ristabilire l'operatività nel sito alternativo
- Erogare i servizi di produzione dal sito alternativo
- Attivare l'operatività nel sito primario