SERVIZIO PER L’INFORMATICA GENERALE

E L’INGEGNERIA CLINICA

AZIENDA ULSS N. 6 “VICENZA”

PIANO DI CONTINUITA’ OPERATIVA E DISASTER RECOVERY

Versione e Data	Titolo	Redatto da:	Verificato da:	Approvato da:
ver. 1 del x/xx/xxxx	Piano di Continuità Operativa e Disaster Recovery			

Sommario

1 Obiettivi del Piano di Continuità Operativa e Disaster Recovery

Obiettivo del presente documento è quello di definire l'organizzazione, le procedure ed i mezzi tecnici che permettano all'Amministrazione di ripristinare i propri servizi IT in caso di interruzioni di qualunque natura, per cui si rende necessario invocare il Piano di Continuità Operativa (di seguito indicato con PCO) e Disaster Recovery.

Il PCO ha la finalità di:

o Gestire un completo e definitivo ripristino dell'operatività in caso di disastro;

o Reagire agli eventi nel modo più tempestivo possibile;

o Stabilire un flusso di comunicazione efficiente in tempi brevissimi in caso di emergenza.

In particolare, la Continuità Operativa comprende fra le attività e soluzioni possibili il "Disaster Recovery", che più propriamente riguarda gli accorgimenti organizzativi e le soluzioni tecniche, organizzative e procedurali adottate per garantire il ripristino dello stato del Sistema Informatico (o parte di esso) per riportarlo alle condizioni di funzionamento e di operatività antecedenti ad un evento disastroso.

Nei paragrafi seguenti verrà quindi presentata la situazione attuale del Sistema Informatico Aziendale e le soluzioni adottate per garantire in particolare la Continuità Operativa ma anche il Disaster Recovery, procedura per la quale sono in previsione diverse attività di implementazione così come previsto dal piano degli investimenti per l'anno 2015.

1.1 Definizioni ed abbreviazioni

- *Continuità Operativa/Business Continuity (CO/BC)*: l'insieme delle attività e delle politiche adottate per ottemperare all'obbligo di assicurare la continuità del funzionamento dell'organizzazione; è parte integrante dei processi e delle politiche di sicurezza e di un'organizzazione.

- *Continuità Operativa ICT (CO)*: la capacità di un organizzazione di adottare - per ciascun processo critico e per ciascun servizio istituzionale critico erogato in modalità ICT, attraverso

accorgimenti, procedure e soluzioni tecnico-organizzative - misure di reazione e contenimento ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi e funzioni istituzionali. Il processo ICT è un caso tipico di processo critico.

- *Disaster recovery (DR*): nell'ottica dell'art. 50bis del CAD, l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate.

- *Piano di Continuità Operativa ICT (PCO)*: Documento operativo che descrive tutte le attività e modalità finalizzate al ripristino delle funzionalità ICT, a seguito di un evento negativo di significativa rilevanza, che determini l'indisponibilità dei servizi classificati come "critici"; per una realtà di dimensioni limitate, soprattutto sotto il profilo ICT, il Piano di Continuità Operativa ICT e il Piano di DR possono coincidere ma dovrà comunque essere presente la componente dedicata al Disaster Recovery. In realtà particolarmente complesse, all'opposto, il piano di continuità può essere solo un documento di primo livello, cui vanno associati, per esempio, documenti di secondo livello, quali procedure relative a servizi e/o sistemi specifici (ad esempio il Piano di Disaster Recovery) e finanche documenti di terzo livello, per esempio sotto la forma di istruzioni di lavoro che riportano le indicazioni operative specifiche;

- *Piano di Disaster Recovery (PDR/DRP):* Documento operativo che descrive tutte le attività necessarie a garantire, a fronte di un evento negativo di significativa rilevanza, che determini l'indisponibilità delle funzioni ICT a supporto dei servizi definiti "critici", il ripristino delle stesse, entro un arco temporale predefinito, tale da rendere, il più possibile, minime le interruzioni nell'erogazione dei servizi. Si evidenzia che il PDR/DRP è la sezione del PCO che descrive le attività di ripristino del sistema informativo; costituisce parte integrante del PCO e stabilisce le misure tecniche ed organizzative per assicurare l'erogazione dei servizi classificati come critici (e delle procedure e applicazioni informatiche correlate) tramite le risorse hw, sw e di connettività presso un CED alternativo a quello/quelli di produzione.

- *RPO: Recovery Point Objective,* indica la perdita dati tollerata: 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 un evento imprevisto.

- *RTO: Recovery Time Objective,* indica il tempo di ripristino del servizio: è la durata di tempo 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;

2 Soluzioni adottate per la Continuità Operativa e Disaster Recovery

2.1 Analisi del livello di criticità dei sistemi

Affinché una organizzazione possa rispondere in maniera efficiente ad una situazione di emergenza sui propri sistemi e impianti, devono essere analizzati:

- I possibili livelli di disastro,
- La criticità dei sistemi/ delle applicazioni.

Per una corretta applicazione del concetto di Business Continuity e Disaster Recovery, i sistemi devono essere classificati secondo le seguenti definizioni:

- *Vitali - livello di criticità: ALTA*

Le relative funzioni possono essere svolte manualmente, ma solo per un breve periodo di tempo. Vi è una discreta tolleranza all'interruzione, conseguentemente il costo di una interruzione è inferiore, anche perché queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).

- *Delicati - livello di criticità: MEDIA*

Queste funzioni possono essere svolte manualmente, a costi tollerabili, per un lungo periodo di tempo. Benché queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.

- *Non - critici - livello di criticità: BASSA*

Le relative funzioni possono rimanere interrotte per un lungo periodo di tempo, con un modesto, o nullo, costo per l'azienda, e si richiede un limitato (o nullo) sforzo di ripartenza quando il sistema viene ripristinato.

2.2 Soluzioni di Continuità Operativa e Disaster Recovery

Per garantire la Continuità Operativa e il Disaster Recovery delle procedure in uso presso questa Amministrazione lo scrivente Servizio per l'Informatica Generale ha adottato, tramite i propri fornitori, una serie di misure diversificate a seconda delle procedure e dei vari applicativi utilizzati dagli utenti.
In particolare, per l'attività di Disaster Recovery sono stati programmati diversi interventi ad integrazione di quanto attualmente implementato, così come riportato all'interno del piano investimenti presentato per l'anno corrente.

Nel capitolo successivo si riporta un elenco delle varie procedure, applicativi e sistemi informatici in uso presso questa Azienda, con indicazione, ad esempio, della Ditta fornitrice e della dislocazione (se interna al CED, extra CED O in Data Center) ma in particolare del corrispondente livello di criticità, in termini di impatto sull'organizzazione aziendale, e della presenza o meno di una soluzione di Continuità Operativa e Disaster Recovery.

A seguire, si allegano alcune schede riassuntive in cui si analizzano i sistemi installati presso questa Azienda nonché, in alcuni casi, i possibili sviluppi futuri in termini di tecnologie e nuovi flussi per la gestione delle procedure di Continuità Operativa e Disaster Recovery.

3 Procedure, applicativi e sistemi informatici in uso presso l'Azienda Ulss n.6 di Vicenza

Vedi Tabella Sistemi Aziendali

3.1 Allegati

- Allegato 1: Ditta AGFA - Analisi installato e prospettive future del progetto RIS PACS dell'ULSS6 di Vicenza;
- Allegato 2: Ditta SIGMA - Server Sigma e Data center**;**
- Allegato 3: Ditta Siemens – Procedura di Backup TDSynergy;
- Allegato 4: Ditta Matika – Soluzione infrastrutturale in uso presso l'Azienda Ulss 6 "Vicenza".