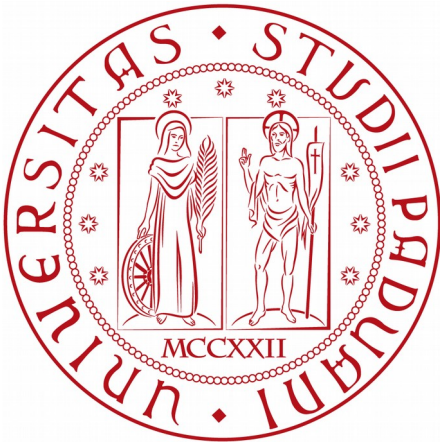
Università degli studi di Padova



Corso di Amministrazione di Sistema

Pecile Francesco 1120771 studente Triennale di Informatica

Piano di contingenza IT sviluppato sulla base di un capitolato dell'ASL di Piacenza

Tabella dei contenuti

2. RaN- Cold Standby
3. RaN- Warm standby
4. RaN- Hot Standby

Allegato: Elenco delle attrezzature informatiche aziendali

1. Computer Aziendali
2. Stampanti Aziendali;
3. Server;
4. Librerie di backup;
5. Linee telefoniche;
6. applicativi aziendali;

Capitolo 1 Introduzione

1.1 Scopo del documento

La componente IT di un contingency plan è il processo di assicurare che le funzioni essenziali di un dipartimento IT possano essere mantenute nonostante l'avvenimento di incidenti ed emergenze.
In questo caso sarà preso in considerazione il dipartimento IT della ASL di Piacenza,modellato secondo le richieste fatte nel capitolato.

In questo documento si andranno quindi a delineare le linee guida e strategie atte a raggiungere 4 obiettivi:

1. Identificare:
    1. Servizi e operazioni fondamentali al funzionamento del business;
    2. Il personale,equipaggiamento,strumenti e record necessari allo svolgimento del servizio;
2. Mantenere disponibili e operative queste due categorie identificate durante i momenti di crisi. Per fare ciò è necessario identificare quali sono tutti i possibili incidenti e definire piani specifici. I procedimenti descritti sono pensati per soddisfare tutte le eventualità del caso ma anche a fornire linee guida per avvenimenti non approfonditi nel dettaglio.
3. Porre degli obiettivi verso i quali programmare il ripristino al loro stato originale dei servizi fondamentali,ritornando alla situazione normale pre-crisi;
4. Identificare ogni processo richiesto e documentare tutti gli step fatti,assieme allo staff e risorse necessarie a completare il lavoro. Sviluppando un piano per ogni singola area e per tutta l'organizzazione;

Più specificamente si andranno a delineare metodi di mantenimento e recupero dati, al fine di mantenere una business continuity e data availability/integrity costante.

Il piano di contingenza informatico si articola su quattro filoni di analisi:

- Impatto sul business (business impact analysis);
- Pianificazione della risposta all'incidente (incidente response plannig);
- Pianificazione del recupero del disastro (Disaster Recovery Planning);
- Pianificazione della continuità del Business (Business Continuity Planning).

Questione fondamentale è che le procedure avviate in caso di crisi siano cost-effective e portino valore economico all'attività, il quale si manifesta nel risparmio delle spese che si verrebbero a creare a fronte di un disastro di tale livello da compromettere il servizio procurato dall'azienda ai suoi clienti.
Questa caratteristica non sarà però approfondita nel dettaglio per incidenti organizzativi(mancanza di un addetto allo studio "economico" del piano)le strategie proposte saranno quindi quelle essenziali e fondamentali per mantenere una corretta qualità del servizio, restando in una spesa medio-alta pensando ad un dipartimento IT che riceve un discreto quantitativo di fondi (visto che opera nell'importante area sanitaria).
Questo documento vuole infine dimostrare che l'avere un efficace Disaster Recovery Plan aiuta anche ad avere una riduzione dei rischi e ad aumentare l'efficienza generale dell'azienda.

1.2 Applicabilità(perimetro)

Identifichiamo le aree essenziali allo svolgimento delle operazioni lavorative

Nome unità	Processo	Priorità(1 valore massimo 5 minimo)	Dipende da	Richiesta da
Uffici	Operazioni IT	2	Funzionamento zona di lavoro/presenza dipendenti Funzionamento infrastrutturale	Dipendenti IT
Call Center	Help desk Ricezione Chiamate	1	Funzionamento zona di lavoro/presenza dipendenti Funzionamento infrastrutturale	Clienti
Area Server	Ospitare i Server	1	Manutenzione e controllo periodico Funzionamento infrastrutturale	Servizi Web Based
Magazzino	Deposito generico	3	Personale Funzionamento infrastrutturale	Tutto il complesso lavorativo
Area Generatore Elettrico	Fornire elettricità a tutto il complesso	1	Contrattore energia elettrica/manutenzione	Tutto il complesso lavorativo
Local Area Network	Collegare tutti i sistemi IT del complesso	1	Manutenzione linee	Tutto il complesso lavorativo

Hot site	Recovery	1	Personale Funzionamento infrastrutturale	Dipartimento

3 BIA

3.1 Identificazione dei sistemi IT

1. Computer Aziendali
2. Stampanti Aziendali;
3. Server;
4. Librerie di backup;
5. Linee telefoniche;
6. applicativi aziendali;
7. LAN/WAN;

Le informazioni dettagliate dei sistemi IT sono date nell'allegato: Elenco delle attrezzature informatiche aziendali.

Identificazione servizi IT

1. Gestione del ciclo di vita della postazione di lavoro (Desktop Lifecycle Services)
    1. Installazione
        1. Consegna, assemblaggio, sistemazione delle apparecchiature informatiche sugli arredi a disposizione dell'utente di destinazione con il collegamento fisico delle apparecchiature alla rete dati mediante al fornitura del cavo di collegamento dalla scheda di rete alla presa di cablaggio per l'accesso fisico alla rete;
        2. Configurazione dei parametri di sistema al fine di consentire il corretto utilizzo dei servizi base disponibili sulla rete aziendale secondo quanto indicato dall'U.O. Sistemi Informativi e Telecomunicazioni, dell'autenticazione utente in Active Directory aziendale e degli indirizzi di posta elettronica resi disponibili all'utente e dove necessario dei parametri di accesso alla rete aziendale mediante dispositivi wireless;
        3. Installazione e configurazione della suite Microsoft Office, secondo le indicazioni fornite dall'U.O;
        4. Installazione di uno o più applicativi aziendali, della configurazione per l'accesso corretto alle funzioni Terminal Server o web services e di tutti i componenti software, dati utente, archivi e dei driver utili per il completo e corretto utilizzo dell'applicativo e dei dispositivi hardware necessari e delle componenti software a protezione da virus informatici e codici maligni nonché del software di inventariazione aziendale;

5. Installazione e configurazione dei software di sincronizzazione e di gestione dei dispositivi di telefonia mobile (cellulari, palmari, smartphone, connect card, ecc..);
6. Apposizione sul bene consegnato del numero d'inventario aziendale;
7. Consegna, se disponibili, all'utente destinatario o al suo responsabile dei manuali e dei CD software a corredo dei beni consegnati ed esecuzione dei test di buon funzionamento per l'accettazione, da parte dell'utente destinatario o del suo responsabile, dei dispositivi hardware e software consegnati;
8. Registrazione dei dati relativi ai beni consegnati, mediante l'impiego dell'apposito software d'Inventario (ambiente software Syntech) che è installato su ogni personal computer dell'Azienda;
9. Recupero dei materiali d'imballo e loro smaltimento secondo la normativa vigente;
10. Certificazione del buon esito dell'esecuzione de tutte le attività eseguite, compreso l'avvenuto ritiro dei materiali d'imballo, firmata dal tecnico esecutore e dall'utente destinatario o dal suo responsabile.

2. Movimentazione
    1. Esecuzione a preventivo delle azioni (copie di salvataggio) utili a protezione dei dati utente quali messaggi di posta elettronica, rubrica personale di Outlook, file e delle configurazioni dall'apparecchiatura informatica mediante sistemi e supporti messi a disposizione dalla ditta aggiudicataria;
    2. Disinstallazione delle apparecchiature informatiche dalla sede di origine (edificio, ufficio, stanza);
    3. Imballo delle apparecchiature informatiche in modo da non causare danno durante la fase di trasporto;
    4. Trasporto delle apparecchiature nella sede di destinazione (edificio, ufficio, stanza);
    5. Installazione delle apparecchiature informatiche nella sede di destinazione (edificio, ufficio, stanza) con collegamento fisico delle apparecchiature alla rete dati mediante al fornitura del cavo di collegamento dalla scheda di rete alla presa di cablaggio per l'accesso fisico alla rete;
    6. Configurazione del sistema al fine di consentire il corretto utilizzo dei servizi base disponibili sulla rete aziendale secondo i parametri della nuova sede (edificio, ufficio, stanza), dell'autenticazione utente in Active Directory aziendale e degli indirizzi di posta elettronica resi disponibili all'utente e dove necessario dei parametri di accesso alla rete aziendale mediante dispositivi wireless;
    7. Registrazione dei dati relativi ai beni consegnati;
    8. Recupero dei materiali d'imballo e loro smaltimento secondo la normativa vigente;
    9. Certificazione del buon esito dell'esecuzione di tutte le attività eseguite, compreso l'avvenuto ritiro dei materiali d'imballo, firmata dal tecnico esecutore e dall'utente destinatario o dal suo responsabile;
    10. Distruzione dei dati di salvataggio preventivamente eseguiti.
3. Aggiunta
    1. Esecuzione a preventivo delle azioni (copie di salvataggio) utili a protezione dei dati utente quali messaggi di posta elettronica, rubrica personale di Outlook, file e delle configurazioni dall'apparecchiatura informatica mediante sistemi e supporti;
    2. Installazione e configurazione di nuovi software e/o applicativi aziendali;
    3. Installazione e configurazione di nuove realease software e/o applicativi aziendali;

4. Assemblaggio dei nuovi dispositivi hardware, sistemazione sugli arredi mobili dell'utente di destinazione e loro installazione e configurazione;
5. Apposizione sui dispositivi hardware consegnati del numero d'inventario aziendale;
6. Consegna, se disponibili, all'utente destinatario o al suo responsabile dei manuali e dei CD software a corredo dei beni consegnati ed esecuzione dei test di buon funzionamento per l'accettazione, da parte dell'utente destinatario o del suo responsabile, dei dispositivi hardware e/o software consegnati;
7. Registrazione dei dati relativi ai beni consegnati, mediante l'impiego dell'apposito software d'Inventario (ambiente software Syntech) che è installato su ogni personal computer dell'Azienda;
8. Recupero dei materiali d'imballo e loro smaltimento secondo la normativa vigente o se concordato il trasporto dei materiali d'imballo nel luogo indicato;
9. Certificazione del buon esito dell'esecuzione di tutte le attività eseguite, compreso l'avvenuto ritiro dei materiali d'imballo, firmata dal tecnico esecutore e dall'utente destinatario o dal suo responsabile;
10. Distruzione dei dati di salvataggio preventivamente eseguiti.

4. Cambiamento
    1. Esecuzione a preventivo delle azioni (copie di salvataggio) utili a protezione dei dati utente quali messaggi di posta elettronica, rubrica personale di Outlook, file e delle configurazioni dall'apparecchiatura informatica mediante sistemi e supporti messi a disposizione dalla ditta aggiudicataria;
    2. Per aggiornamenti software:
        1. Installazione e configurazione di nuove versioni di software applicativo aziendale e suoi componenti e/o di drive e/o di Service Pack sulla postazione.
    3. Per aggiornamenti hardware
        1. Installazione e configurazione dei nuovi dispositivi hardware sulla postazione di lavoro.
    4. Per aggiornamento della postazione di lavoro
        1. Assemblaggio e sistemazione delle apparecchiature sugli arredi mobili dell'utente di destinazione con collegamento fisico delle apparecchiature alla rete dati mediante al fornitura del cavo di collegamento dalla scheda di rete alla presa di cablaggio per l'accesso fisico alla rete;
        2. Installazione della suite Microsoft Office;
        3. Configurazione dei parametri di sistema al fine di consentire il corretto utilizzo dei servizi base disponibili sulla rete aziendale, dell'autenticazione utente in Active Directory aziendale e degli indirizzi di posta elettronica resi disponibili all'utente e dove necessario dei parametri di accesso alla rete aziendale mediante dispositivi wireless;
        4. Installazione di uno o più applicativi aziendali,della configurazione per l'accesso corretto alle funzioni Terminal Server o web services, qualora questi lo richiedano, di eventuali software d'emulazione per l'accesso ai servizi host disponibili sulla rete aziendale o sulla rete della Regione Emilia-Romagna, e di tutti i componenti software, dati utente, archivi e dei driver utili per il completo e corretto utilizzo dell'applicativo e dei dispositivi hardware necessari e delle componenti software a protezione da virus informatici e codici maligni nonché del software di inventariazione aziendale (Syntech);

5. Installazione e configurazione dei software di sincronizzazione e di gestione dei dispositivi di telefonia mobile (cellulari, palmari, smartphone, connect card, ecc..) qualora fosse necessario;
6. ripristino nelle posizioni originarie dei file utente comprese i file di posta personali;
7. Consegna, se disponibili, all'utente destinatario o al suo responsabile dei manuali e dei CD software a corredo dei beni consegnati ed esecuzione dei test di buon funzionamento per l'accettazione, da parte dell'utente destinatario o del suo responsabile, dei dispositivi hardware e/o software consegnati;
8. Apposizione sul nuovo dispositivi hardware consegnato del numero d'inventario aziendale;
9. Registrazione dei dati relativi ai beni consegnati,mediante l'impiego dell'apposito software d'Inventario (ambiente software Syntech) che è installato su ogni personal computer dell'Azienda;
10. Recupero dei materiali d'imballo e loro smaltimento secondo la normativa vigente;
11. Certificazione del buon esito dell'esecuzione de tutte le attività eseguite, compreso l'avvenuto ritiro dei materiali d'imballo, firmata dal tecnico esecutore e dall'utente destinatario o dal suo responsabile;
12. Distruzione dei dati di salvataggio preventivamente eseguiti.

5. Rimozione
    1. Esecuzione a preventivo delle azioni (copie di salvataggio) utili a protezione dei dati utente quali messaggi di posta elettronica, rubrica personale di Outlook, file e delle configurazioni dall'apparecchiatura informatica mediante sistemi e supporti messi a disposizione dalla ditta aggiudicataria;
    2. Eliminazione dei parametri di sistema al fine di consentire il corretto utilizzo dei servizi base disponibili sulla rete aziendale, dell'autenticazione utente in Active Directory aziendale e degli indirizzi di posta elettronica resi disponibili all'utente e dove presenti dei parametri di accesso alla rete aziendale mediante dispositivi wireless, eliminazione di tutti i software presenti sul dispositivo che non trattasi di sistema operativo o sui componenti ed di tutti i dati utente;
    3. Ritiro, se disponibili, dall'utente destinatario o dal suo responsabile dei manuali e dei CD software a corredo dei beni ritirati e disinstallazione fisica dei dispositivi
    4. Imballaggio dei dispositivi rimossi e loro trasporto al Magazzino aziendale
    5. Certificazione del buon esito dell'esecuzione de tutte le attività eseguite, firmata dal tecnico esecutore e dall'utente destinatario o dal suo responsabile;
    6. Distruzione dei dati di salvataggio preventivamente eseguiti.
6. Smaltimento

2. Manutenzione Hardware e Manutenzione Software
    1. Hardware:Il servizio richiesto deve garantire l'esecuzione di tutte le attività di manutenzione hardware on-site sui computer e le periferiche ad esso collegate quali video, tastiera, mouse, penne ottiche, lettori barcode, modem, stampante, scanner, ecc. e le stampanti di rete;
    2. Software
        1. bonifica del personal computer da virus informatici o da altri software maligni;

    2. installazione di patch o fix attinenti il sistema operativo o suoi componenti ed alla suite di Microsoft Office o suoi componenti;
    3. ripristino e/o correzione delle configurazioni di sistema al fine di consentire il corretto utilizzo dei servizi base disponibili sulla rete aziendale, dell'autenticazione utente in Active Directory aziendale e degli indirizzi di posta elettronica resi disponibili all'utente e dove presenti dei parametri di accesso alla rete aziendale mediante dispositivi wireless;
    4. ripristino e/o correzione dell'installazione del sistema operativo o suoi componenti e dell'installazione della suite di Microsoft Office o suoi componenti;
3. Servizio di Help Desk I livello (pronta assistenza agli utenti sui sistemi hardware e software di primo livello);
4. Servizio di Help Desk II livello (pronta assistenza agli utenti hardware e software di secondo livello):
    1. posta elettronica
    2. firewall
    3. antivirus
    4. active directory
    5. DNS
    6. office automation
    7. Sistemi Operativi (Windows/Linux)
    8. Microsoft IIS
    9. Apache Software Foundation
    10. software di virtualizzazione (VMWare, Citrix, ecc..)
    11. database (Microsoft/Oracle)
5. Servizio di "Monitoraggio " degli apparati di rete, delle linee dati;
6. Servizio di "Ricezione Chiamate" per le segnalazioni di guasto sui dispositivi telefonici e linee telefoniche;
7. Servizio di "Ricezione Chiamate" per le richieste di assistenza tecniche/informatiche RIS-PACS:
    1. software di gestione RIS
    2. utilizzo della stazione di visualizzazione immagini
    3. modalità di visualizzazione referti/immagini
    4. creazione su memorie magnetiche del referto e immagini dell'esame eseguito da consegnare al paziente
8. Servizio di "Ricezione Chiamate" per le richieste di assistenza su applicativi informatici aziendali;
9. Servizio di Call Center unico;
10. servizio di segreteria telefonica;
11. Service Desk:
    1. Incident Control: gestione del ciclo di vita di tutte le richieste di servizio;
    2. Comunicazione: tenere informato l'utente del progresso del lavoro svolto sulla sua richiesta e di aiutarlo nelle soluzioni.
12. Incident Management:
    1. Rilevare e registrare gli incidenti;
    2. Classificare incidenti;
    3. Fornire all'utente un iniziale supporto;

4. Assegnare una priorità agli incidenti sulla base dell’impatto e dell’urgenza;
5. Studiare gli incidenti e proporre una diagnosi;
6. Risolvere gli incidenti per recuperare i livelli di servizio concordati;
7. Chiudere gli incidenti;
8. Mantenere la proprietà, il controllo, il monitoraggio e le comunicazioni sugli incidenti;
9. Fornire informazioni sulla qualità e sulle operazioni svolte dall’Incident Management.

13. Problem Management:
    1. Analisi delle tendenze;
    2. Indicazioni di azioni mirate;
    3. Fornire informazioni per l'organizzazione.
14. Service Level Management:
    1. garantire che il livello convenuto di tutti i servizi IT sono vengono mantenuti;
    2. favorire il collegamento con l'Incident Management ed il Problem Management per garantire che i livelli e la qualità del servizio siano realizzati secondo quanto concordato;
    3. produrre e mantenere il Service Catalog (l’elenco dei livelli dei servizi IT a disposizione degli utenti) ;
    4. garantire la definizione di adeguati piani di IT Service Continuity a sostegno della continuità dell'attività aziendale;
    5. monitorare e gestire SLA e OLAs;
    6. avviare azioni di miglioramento del servizio;
    7. fornire informazioni sulla qualità e sulle operazioni del Service Level Management;
15. Remote Desktop Control.

3 Valutazioni sul rischio e sulla accettabilità di questo

Il contingency plan deve prevedere 3 tipi di danni al sistema lavorativo:

1. Chiusura di una facility(ad esempio danni ad un edificio)
2. Riduzione della forza lavoro(influenze particolarmente contagiose)
3. Technological equipment or systems failure(incidenti relativi ai sistemi IT)

Potenziale Disastro	Livello di Probabillità (1 alto 5 basso)	Livello di impatto	Descrizione sintetica delle conseguenze e possibili rimedi (sarà ben approfondita nei capitoli successivi)
Alluvione	3	4	Grave se tutto l'equipaggiamento critico è locato al primo piano
Incendio	3	4	Sistema di soppressione incendi installato in tutte le aree in presenza di computer.Rilevatore di fumo installati in tutti i piani.
Tornado	5		Chiusura della facility per potenziale pericolo ai dipendenti
Tempeste elettriche	5	4	Protezione dei cavi elettrici
Terrorismo	5		
Atti di sabotaggio	5		
Danneggiamento rete elettrica	3	4	Array UPS ridondante assieme ad un generatore standby testato settimanalmente e monitorato da remoto 24/7.Monitoraggio UPS.
Perdita di comunicazione tra network services	4	4	Ridondanza LAN e WAN
Mancanza di dipendenti(influenze stagionali,assenze non avvisate,scioperi)	2	4	Spostamento del carico di lavoro URGENTE ad altri dipendenti
Danni alla sala server	3	5	Server e librerie di Backup.Monitoraggio server 24/7
Incidenti relativi al magazzino	4	3	Magazzino di backup(per oggetti prelevati frequentemente
Mancanza di supporto software per cause esterne	4	5	Contrarre un nuovo contratto con un altra ditta di fornitura software
Danni al generatore elettrico/perdita di corrente elettrica	3	5	Generatore d'emergenza
Scorretta update della base di dati SQL	2	3	Librerie SQL di backup
Virus,malware	3	4	Suite di protezione informatica
Incidenti minori(danni al pc ed equipaggiamenti base)	1	1	Risolvibile dal personale

4 Tempi

I servizi di Gestione del ciclo di vita della postazione di lavoro, di Manutenzione Hardware e Manutenzione Software, ed il Servizio di Help Desk di II livello, fatto salvo proposte migliorative, dovranno essere disponibili dal Lunedì al Venerdì dalle ore 8,00 alle ore 13,00 e dalle ore 14,00 alle ore 18,00 ed il Sabato dalle 8,00 alle 14,00. Sono esclusi i giorni festivi.

Il Servizio di Call Center unico (in particolare per quanto concerne il Servizio di Ricezione Chiamate per le segnalazioni di guasto sui dispositivi telefonici e linee telefoniche, il Servizio di "Ricezione Chiamate" per le richieste di assistenza tecniche/informatiche RIS-PACS ed il Servizio di "Ricezione Chiamate" per le richieste di assistenza su applicativi informatici aziendali), fatto salvo proposte migliorative, dovrà essere disponibile dal Lunedì al Venerdì dalle ore 7,30 alle ore 20,30 ed il Sabato dalle 8,00 alle 14,00. Sono esclusi i giorni festivi. Il servizio si farà carico di ricevere tutte le telefonate e di attivare i tecnici incaricati oppure di passarle, quelle di competenza, al Servizio di Help Desk di I livello.
Il Servizio di Help Desk di I livello ed il Servizio di monitoraggio degli apparati di rete e delle linee dati fatto salvo proposte migliorative, dovrà essere disponibile dal Lunedì al Venerdì dalle ore 8,00 alle ore 13,00 e dalle ore 14,00 alle ore 18,00 ed il Sabato dalle 8,00 alle 14,00. Sono esclusi i giorni festivi.

Definizione dei 4 tipi di tempi:

(1) apertura richiesta d'Intervento: Il database dell'applicativo di Service Support di cui al Lotto 2 riporta gli identificativi in chiaro di data e d'ora in cui è stato aperto un nuovo caso o incidente.
(2) tempo di reazione: È l'intervallo di tempo che intercorre dal momento in cui è aperto un nuovo incidente al momento in cui la ditta aggiudicataria ne inizia il trattamento attivando le opportune risorse e procedure di diagnostica e recovery.
(3) tempo di intervento: È l'intervallo di tempo che intercorre dall'apertura dell'incidente al momento in cui la ditta aggiudicataria inizia ad operare sulle componenti guaste o malfunzionanti ed alla risoluzione del problema segnalato.
(4) tempo di ripristino: È l'intervallo di tempo che intercorre dall'apertura dell'incidente all'istante in cui il guasto è rimosso e il sistema riprende a funzionare correttamente ai pattuiti livelli qualitativi e di servizio.

Gli intervalli di tempo non sono cumulabili, ovvero tutti gli intervalli sono sempre misurati dal primo evento che è l'apertura richiesta d'Intervento.
La ditta deve garantire i seguenti requisiti d'affidabilità:
(1) tempo massimo di reazione <= 30 minuti
(2) tempo massimo di intervento <= 4 ore lavorative
(3) tempo massimo di ripristino <= 8 ore lavorative

Il dipartimento è tenuto, nel caso in cui la riparazione delle attrezzature quali personal computer e stampanti comporti tempi superiori alle 8 ore lavorative, a fornire la sostituzione dell'apparecchiatura con altra equivalente per tutto il tempo di durata dell'intervento. Per tutta la

durata del contratto la sostituzione temporanea dell'apparecchiatura dovrà essere garantita sino un massimo del 10% del totale di personal computer inventariati e sino ad un massimo del 10% del totale di stampanti inventariate.

5 Opzioni di Ripristino

Strategie di backup

Questo capitolo descrive nel dettaglio tutte le strategie di backup per PC,LAN,WAN,SERVER

Backup PC
Il backup dei dati da PC può essere implementato in vari modi:

1. Floppy disk drives,questi sono presenti di default all'acquisto di desktop PC e rappresentano la scelta più economica,infatti sono lenti e non offrono molta capacità di storage;
2. Tape Drives,questi non sono molto usati per desktop PC ma sono un'opzione data la loro elevata capacità di storage,sono automatizzati e richiedono una applicazione di backup da terze parti o delle applicazioni di backup del sistema operativo;
3. Removable Cartridges,sono più costose dei floppy disk però sono molto più veloci e la loro portabilità offre molta flessibilità d'uso;
4. CD-ROM standard read only memory;
5. Network storage,I dati salvati su PC networkati possono fare back up usando dischi collegati al network o su network storage devices:
    1. Networked disk,questi sono server con capacità di data storage,il backup viene fatto tramite software di backup e la capacità dipende dalla capacità dei dischi;
    2. Networked storage device,un network backup system può essere configurato per fare backup su PC networkati, il backup può essere fatto partire sia dall'attuale PC o dal sistema di backup;
6. Replication or Synchronization,l'opzione più comune per computer portatili può essere full,incremental e differential;
7. Internet Backup,servizio commerciale che permette agli user di salvare dati in remoto pagando;

Si è deciso di utilizzare buona parte di queste 7 opzioni:

1. Usare una definitive media library,la quale supporta i seguenti benefici:
    1. Provvede le risorse di tutte le applicazioni e raw media da usare nel service restoration e disaster recovery,aumentando quindi le capacità di Availability e service continuity ;
    2. provvede dei metadata records e record delle chiavi di licenza dei software,garantendo un ottimizzato management delle allocazioni software;
    3. Management della release e deployment per tutti i package.
2. Network storage posto nell'edificio principale;
3. Full replication e synchronization dei dati,i quali vengono conservati in un edificio secondario;

Backup Server

Per questo piano di contingenza si è deciso di fare un Incremental Backup.
Le domande a cui bisogna rispondere sono:

1. Dove saranno collocati i dati? In una stanza adibita ad ospitare le librerie di backup posta in un edificio diverso da quello principale,il quale sarà descritto nel capitolo Stabilimento di Contingency;
2. Quali dati dovranno essere salvati? In questo caso il compito del dipartimento IT è quello di supportare l'ASL di Piacenza,quindi la gran parte dei dati di genere medico sono ad alta priorità e confidenzialità;
3. Con quale frequenza saranno condotti i backup ? La frequenza di backup varia a seconda dei dati e metodi usati,verrà descritta nei singoli casi;
4. Chi è autorizzato ad accedere ai media? Sarà descritto nel capitolo Security;
5. Quanto velocemente devono essere recuperati i dati in caso di emergenza? l'urgenza del recupero dei dati varia dal livello di allerta dell'incidente e dal livello di attivazione del piano di contingenza;
6. dove saranno consegnati i dati? I dati saranno consegnati agli direttamente negli uffici nel caos di perdita di dati medici;
7. Chi farà il restore dei dati? Il personale del nostro dipartimento IT,come richiesto da capitolato;
8. Per quanto tempo saranno mantenuti i dati ? I dati di carattere medico(cartelle cliniche,scan radiologiche) saranno mantenute per un tempo indefinito,per poter essere usufruibili anche dopo il decesso di un paziente,invece i dati d'ufficio e supporto alle operazioni saranno mantenuti a discrezione dell'infrastructure management;

La tecnica di data replication utilizzata per i dati critici al mantenimento del business sarà quella Sincrona,questo metodo usa una copia disco a disco e mantiene una replica del database o file system applicanto i cambiamenti al server di replica nello stesso momento in cui queste vengono fatte nel main site, per non degradare le performance.
Con questa tecnica RTO può andare da minuti e varie ore,mentre RPO sarà ridotto grazie alla perdita di lavoro non compiuto.

Backup LAN/WAN

Nel caso di danni ai cavi della LAN,i quali possono essere causati da tagli,interferenze elettromagnetiche,incendi,alluvioni o altri incidenti,si può decidere un certo livello di ridondanza dei cavi. La scelta più cost-effective è quella di installare una 100-megabit cable tra tutti i piani dell'edificio principale,in modo che se il cavo primario della LAN subisse danni abbastanza gravi da renderlo fuori uso,gli host dei vari piani possano continuare a lavorare passando al cavo d'emergenza.
Non verranno installati cavi ridondanti per i singoli computer,ma nel magazzino saranno sempre presenti vari tipi di cavi per riparare gli incidenti più comuni.

Il cavo di emergenza però mantiene operative solo le parti cruciali del business e nel caso di incidenti molto gravi da solo non può garantire la completa sicurezza della LAN,d'altronde bisogna tenere conto che le operazioni non vengono effettuate solo nell'edificio principale.

Per rimediare a ciò è necessario utilizzare un Wireless local area network,questo non richiede cavi e opera su un'infrastruttura diversa dalla LAN,quindi copre gli incidenti e rischi di cui la LAN e affetta.
La WAN però è suscettibile ad altri incidenti,usando segnali radio lascia che i dati possano essere intercettati,creando possibili incidenti di sicurezza.
Per prevenire ciò è necessario usare data encryption e usare un software di monitoraggio,questo inoltre è stato chiesto da capitolato,quindi la soluzione risulta perfetta per la situazione richiesta.

In aggiunta,bisogna considerare i link di comunicazione che connettono le diverse LAN e il fatto che le strategia di contingenza per una WAN sono influenzate dal tipo di dato che passa attraverso il network.
Una WAN che trasmette dati critici,come nel nostro caso(trasmettiamo dati ospedalieri da altissima confidenzialità),richiede una strategia di recovery più robusta da una WAN che connette multiple LAN per semplice resource sharing.
Dobbiamo quindi implementare le seguenti strategie:

1. Link di comunicazione ridondanti. Questi sono necessari nel maneggiamento di dati critici. Per fare ciò utilizziamo un backup link che metterà a disposizione una larghezza di banda ridotta atta a salvare solo i dati critici in una situazione di contingenza. Bisogna prestare attenzione al fatto che i link ridondanti devono essere fisicamente separati e non devono condividere lo stesso path,altrimenti un incidente potrebbe coinvolgere più link ridondanti;
2. Network Service Providers ridondanti,nel nostro caso è necessaria una availability dei dati al 100%,per essere sicuri di ciò è necessario avere un NSP di backup nel caso che il primo abbia un incidente,infine è imperativo stringere contratti con NSP localizzate in luoghi diversi,se una subisce un incidente l'altra deve esserne al sicuro al 100%;
3. Network Connecting Devices ridondanti. Router,switch e firewall ridondanti sono utili per mantenere una alta availability,devices duplicati possono anche aiutare a bilanciare il traffico elevato di dati;

Precisazioni:
L'uso di NSP o ISP ridondanti può portare ad una maggiore vulnerabilità ad attacchi informatici, per fare ciò prima di stipulare il contratto con un NSP di backup è necessario fare un assessment della robustezza della loro piattaforma.

Si è deciso di un usare anche un ISP di backup poiché i dati saranno sempre salvati in locale,quindi nel caso di una perdita di connessione internet i dati critici non saranno persi,si può quindi aspettare che il DRT rimetta in sesto la connessione.
Così facendo il bilanciamento tra availability e security sarà garantito.

Sintesi Backup
La strategia scelta consiste in un fully mirrored recovery site (hot site) situato in un edificio diverso da quello principale.
Questa strategia richiede una manutenzione costante ma offre uno switch istantaneo tra il live site e il backup site in caso di necessità.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	Fully mirrored recovery site
Tech Support - Hardware	Fully mirrored recovery site
Tech Support - Software	Fully mirrored recovery site
Facilities Management	Fully mirrored recovery site
Email	Fully mirrored recovery site
Disaster Recovery	Fully mirrored recovery site
Finance	Fully mirrored recovery site
Contracts Admin	Fully mirrored recovery site
Warehouse & Inventory	Fully mirrored recovery site
Maintenance Sales	Fully mirrored recovery site
Human Resources	Off-site data storage facility
Testing Fully Mirrored Recovery site -	Fully mirrored recovery site
Workshop Fully Mirrored Recovery site -	Fully mirrored recovery site
Call Center	Fully mirrored recovery site

Capitolo 2 Infrastruttura IT

Di seguito vengono indicati alcuni concetti che caratterizzano il Sistema Informativo dell'Azienda Unità Sanitaria Locale di Piacenza:
• Reti locali realizzate mediante cablaggio strutturato cat.5, cat.5e o cat.6 intestato su connettori RJ45; il segnale è amministrato mediante dispositivi switch Layer 2 e 3;
• Protocollo in utilizzo TCP/IP;
• Sistema operativo di rete adottato Microsoft Windows;
• Sistemi operativi sui server applicativi sono Microsoft Windows, Linux in diversi dialetti e Unix like;
• I servizi di rete (Deposito dei file, Posta elettronica, DHCP, ecc) sono fruibili dagli utenti via LAN, è in corso la revisione della distribuzione dei servizi per il loro consolidamento su un numero minore di sistemi e di locali tecnici;
• Utilizzo di DHCP in ogni LAN;
• Le applicazioni attualmente in funzione nel Sistema Informativo operano con funzionalità di Terminal Server mentre altre operano in tecnologia Web, in Client/server, in emulazione terminale inoltre esistono applicazioni installate e funzionanti su computer in locale;
• Soluzione firewall adottata CheckPoint;
• Soluzione proxy adottata Microsoft ISA Server 2000;
• Microsoft® Active Directory® Services (ADS) 2003;

I prodotti di Microsoft presenti nei diversi Domini attivati in azienda sono:
• Microsoft Windows Server
• Microsoft ISA Server
• Microsoft Exchange Server
• Microsoft SQL Server
• Microsoft IIS Server

I Servizi base attivi sono:
• Wins
• Active Directory
• DHCP
• DNS
• File Server
• RAS Server
• HTTP
• FTP
• Index Server

I client di rete sono configurati, di base, come segue:
• Windows 2000 Prof. o Windows XP Prof.
• Office 2000 o Office 2003;
• Outlook 2000 o Outlook 2003;
• Microsoft Internet Explorer;
• altri browser richiesti dagli applicativi in uso (ad es. Firefox);
• Software “Monitor Personale” e apposito software d’Inventario (ambiente software Syntech);
• Trend Micro OfficeScan Client;
• Unità disco NTFS;
• Dominio di appartenenza auslpc.net;
• Configurazione dei servizi TCP/IP, compresi collegamenti remoti, VPN, ecc… per il corretto accesso alla rete aziendale sia via cavo che wireless;
• Adobe Acrobat Reader 8;
• Lettore Smart Card reader integrato nella tastiera oppure USB.

In aggiunta a quanto sopra elencato i client potranno inoltre essere dotati dei seguenti software:
• software di sincronizzazione e di gestione dei dispositivi di telefonia mobile:
• Componenti ActiveX per l’utilizzo di applicativi WEB e anche browser diversi da Microsoft Internet Explorer richiesti necessari per l’utilizzo degli applicativi (ad es. Firefox);
• Componente ActiveX per l’utilizzo dell’applicativo DocSuite di Protocollo aziendale;
• Componente ActiveX per l’utilizzo dell’applicativo Siemens MagicWeb di visualizzazione delle immagini di diagnostica radiologica.

Al fine di prevenire azioni non consentite da parte dell’utente utilizzatore cel computer è previsto che il “domain user account” di norma deve appartenere al local groups “Users” e diverse assegnazioni devono essere fatte solamente dietro indicazione dell’U.O. Sistemi Informativi e Telecomunicazioni.

Gli utenti possono accedere a risorse condivise sui server (directory, file e/o stampanti) stabilite e predisposte centralmente dall'U.O. Sistemi Informativi e Telecomunicazioni.

La gestione degli account di rete avviene in modo centralizzato e manuale per tutti i dipendenti, fornitori, consulenti esterni ed account di servizio.

I client di rete usufruiscono dei seguenti servizi base:
• file sharing utente;
• file sharing di gruppo;
• printer sharing;
• messaggistica e collaborazione;
• navigazione internet;
• accesso ad applicativi terminal server, locali, client/server o web/based;
• accesso alla intranet aziendale.

Come client sono presenti anche palmari con S.O. Microsoft Windows CE che si collegano alla rete aziendale grazie ad un'infrastruttura Wi-Fi realizzata con componenti del produttore Trapeze Networks™ ed autenticati localmente o mediante Radius Server. Questi dispositivi, di norma, sono impiegati per accedere ad applicazioni terminal server.

Le funzioni di protezione dai virus informatici sui client e sui server sono assicurate mediante la NeatSuite di Trend Micro. La suite comprende InterScan Messaging™ Security Suite, ed InterScan™ Web Security Suite, ScanMail™ for Microsoft™ Exchange con eManager, e ServerProtect™ per Microsoft Windows per sevres di classe enterprise ed OfficeScan™ per desktop e server.

Le funzioni di salvataggio e recovery sono eseguite tramite i prodotti di Computer Associates BrighStor ARCserve Backup. Le funzioni implementate sono riferibili ai dati presenti sui server o sulle storage in SAN ed assicurano da una consolle di gestione la corretta schedulazione, esecuzione e ripristino delle sessioni di salvataggio su server eterogenei cioè con diverso S.O. mediante l'impiego d'opportuni agenti.

Capitolo 3 Personale

3.1 Ruoli

I ruoli in situazioni normali e di crisi Esecuzione delle attività,

Operazioni Normali	Durante una crisi
Livelli di Board(consiglio)	
Avviare la Continuità dei Servizi Informatici, impostare la politica, allocare le responsabilità, indirizzare ed autorizzare	Gestione delle crisi, decisioni aziendali, affari esterni
Senior Management	
Gestire la Continuità dei Servizi Informatici, accettare parti da consegnare, comunicare e mantenere la consapevolezza, integrare in tutta l'organizzazione	Coordinazione, indirizzamento e arbitrati, autorizzazione delle risorse
Junior Management	
Intraprendere l'analisi della Continuità dei Servizi Informatici, definire parti da consegnare, contattare i servizi, gestire i test e le assicurazioni	Richiamo, leadership del team, gestione del sito, collegamento e rapporto
Supervisori e Staff	
Sviluppare parti da consegnare, negoziare i servizi, eseguire i test, sviluppare ed eseguire i processi e procedure	Esecuzione delle attività, partecipazione ai team, collegamenti

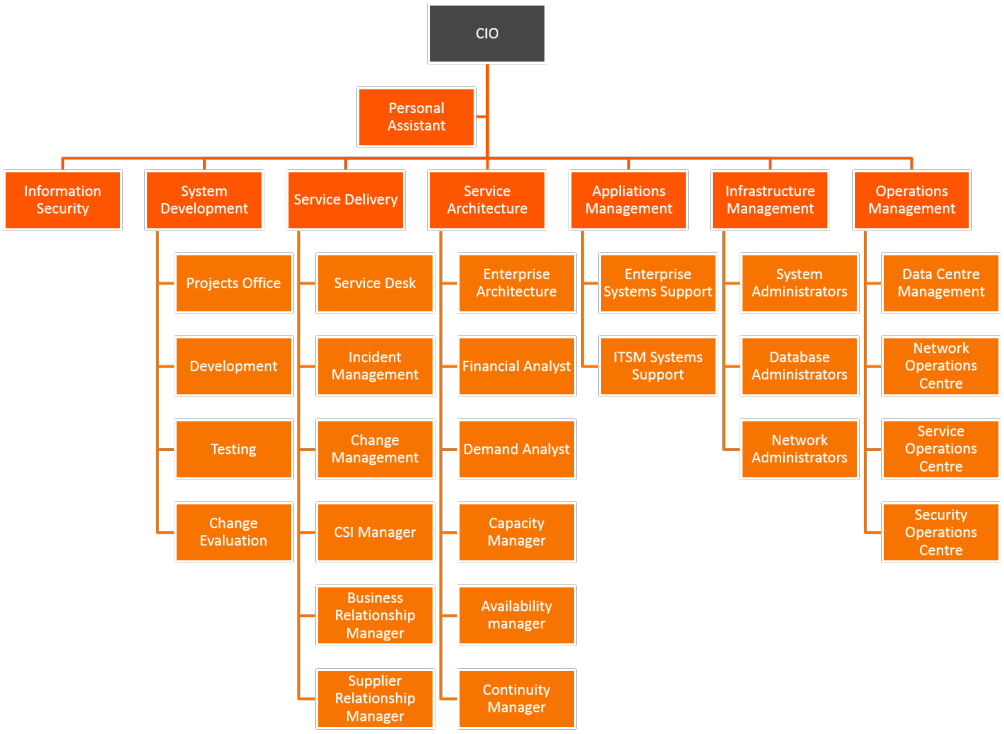
3.2 Contatti

Contatti personale chiave (nominativi inventati per riempire lo spazio,dato che nel capitolato non erano presenti)

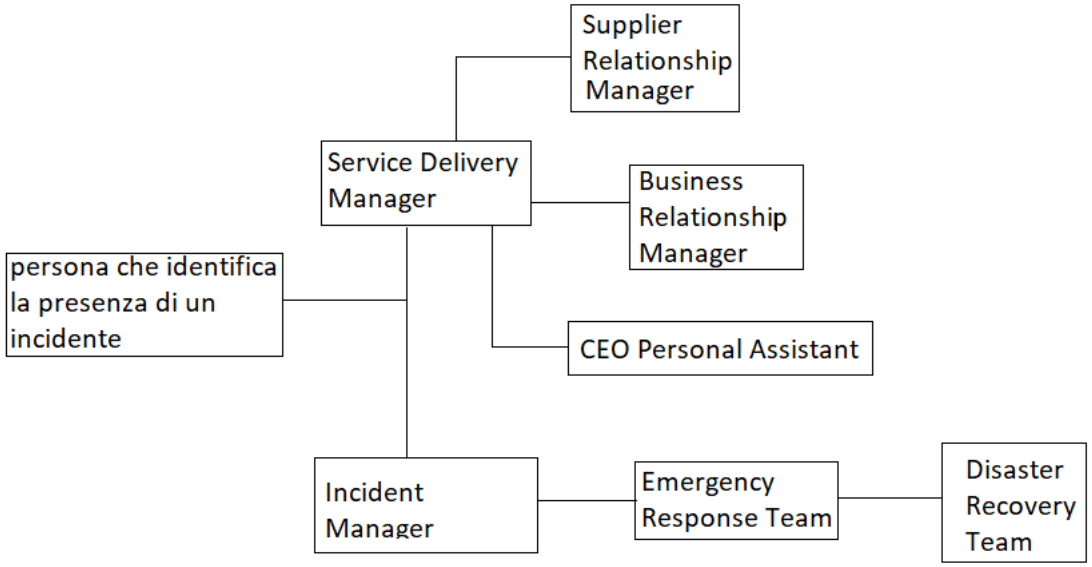
Name, Title	Contact Option	Contact Number
Marco Donati CIO	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
Filippo Giusti CIO assistant	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
Alessia Salvati Information security	Work	

Name, Title	Contact Option	Contact Number
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
Andrea Pecile System Development	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
Salvatore Caputi Service Delivery	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
Giula Pascolo Service Architecture	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
Marco Barberi Applications Manager	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
Davide Fisi Infrastructure manager	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
Aldo Conti Operations Manager	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	

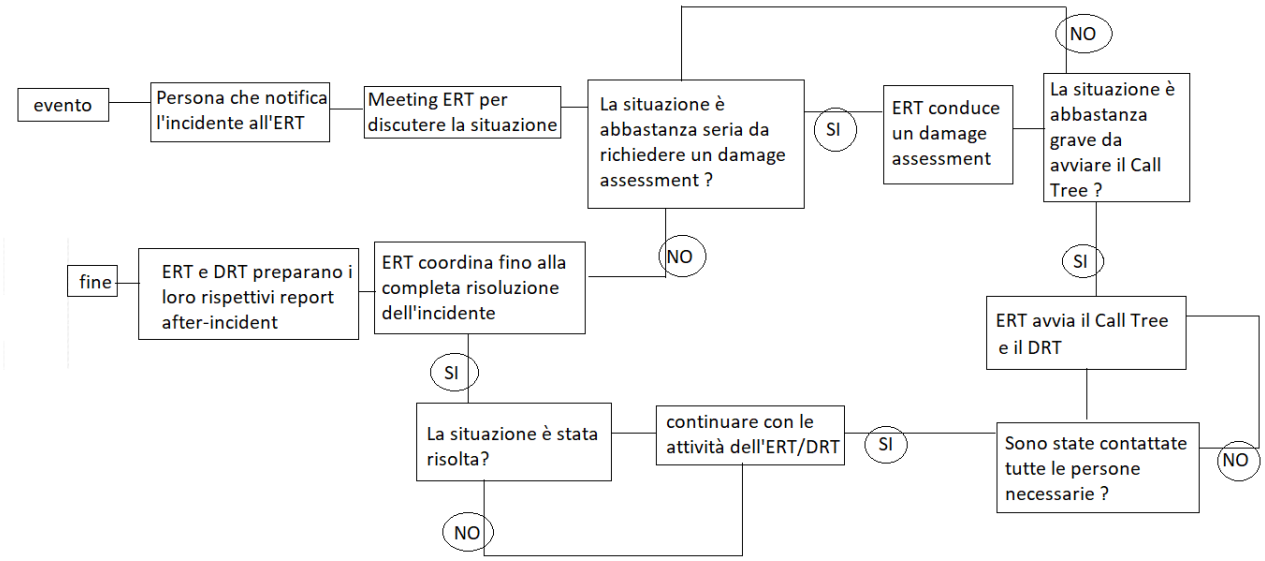
3.3 Schema Gerarchia aziendale



3.4 Calling Tree



Esecuzione del Call Tree



3.5 Contatti Esterni

Nome,Titolo	Opzioni di Contatto	Informazioni di contatto
Manager di Proprietà		
Marco Colussi		
	Work	
	Mobile	
	Home	
	Email Address	
Compagnia Elettrica		
Luca Collini	Work	
	Mobile	
	Home	
	Email Address	
Telecom Carrier 1		
Mirko Foschiani	Work	
	Mobile	
	Fax	
	Home	
	Email Address	
Telecom Carrier 2		
Eleonora Fiore	Work	
	Mobile	
	Home	
	Email Address	
Fornitore Hardware		
Leonardo Nardone	Work	
	Mobile	
	Emergency Reporting	
	Email Address	
Fornitore Server		
Andrea Nocino	Work	
	Mobile	
	Fax	
	Email Address	
Fornitore Workstation		
Sara Gaspar	Work	
	Mobile	
	Home	
	Email Address	
Fornitore per l’ufficio		
Elena Ninzatti	Work	
	Mobile	
	Home	
	Email Address	
Assicurazione Bancaria		
Amato Dante	Work	
	Mobile	
	Home	
	Email Address	
Sicurezza dei Siti		

Nome,Titolo	Opzioni di Contatto	Informazioni di contatto
Edoardo Alfonso	Work	
	Mobile	
	Home	
	Email Address	
Magazzino		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Generatore Elettrico		
Marco Gasparin	Work	
	Mobile	
	Home	
	Email Address	

3.6 Team

Attivazione dell’ Emergency Response Team

All’avvenimento di un incidente l’Emergency Response Team (ERT) deve essere attivato. L’ERT a tal punto deciderà il livello di emergenza relativo all’incidente e di conseguenza la portata di attivazione del piano di contigenza. Tutti gli impiegati devono possedere le informazioni di contatto relative ai membri dell’ERT da poter usare in caso di incidente.
Le responsabilità dell’ERT sono:

- Rispondere immediatamente ad un possibile incidente e chiamare i servizi di emerge;
- Fare una stima dell’estensione e pericolosità dell’incidente,assieme all’impatto derivato sul business,data center etc etc;
- Decidere quali elementi del Piano di Contingenza debbano essere attivati;
- Stabilire e amministrare il Disaster Recovery team per mantenere attivi i servizi vitali e tornare alla situazione di lavoro normale;
- Assicurarsi che tutti gli impiegati siano notificati e allocare attività e responsabilità come richiesto;

Disaster Recovery Team

Il team sarà contattato e composto dall’ERT.
Potrà essere composto da membri di vari team:

1. Server Recovery Team
2. LAN/WAN Recovery Team
3. Database Recovery Team
4. Network Operations Recovery Team
5. Application Recovery Team
6. Telecommunications Team
7. Hardware Salvage Team
8. Alternate Site Recovery Coordination Team
9. Original Site Restoration/Salvage Coordination Team
10. Test Team
11. Administrative Support Team
12. Transportation and Relocation Team
13. Media Relations Team

14. Legal Affairs Team
15. Physical/Personnel Security Team
16. Procurement Team (equipment and supplies)

La grandezza e complessità di ciascuno di questi team deve essere decisa in un contesto di assunzioni di organico.
I membri del Disaster Recovery Team saranno scelti e aiutati dal personale di questi team,nel contesto di incidente attuale.
Esempio:Nel caso di un incidente relativo alla LAN,l'ERT comporrà il DRT di membri del LAN/WAN recovery team più un responsabile scelto dal senior management aziendale.

Le responsabilità del team includono:
- Stabilire facilities per un emergenza a livello di servizio nel raggio di 2 ore lavorative;
- Rimettere operativi i servizi chiave nel raggio di 4 ore dall'incidente.
- Ristabilire la normale routine di business in 8-24 ore dopo l'incidente;
- Coordinare le attività con il disaster recovery team;
- Fare un report per l'emergency response team;

Staff di Backup

Nel caso in cui un componente del ERT,DRT o un manager senior dovesse mancare,deve esserci un dipendente di backup che lo possa sostuire.
Nel caso il sostituto designato non abbia lo stesso livello di competenze dell'originale membro,esso deve limitarsi ad azioni di notifica e supporto.

Captitolo 5 Amministrazione

5.1 leadership e misure di sicurezza

Le componenti dell IT security descritte nel Contingency Plan supportano gli obiettivi di business Continuity. Da questo risulta che l'attivazione di una qualsiasi parte del Contingency Plan (inclusi Disaster Recovery e Emergency Operations) sia governata dal CIO e dalle procedure documentate per assicurare la Business Continuity.
Dopo l'avvio da parte del CIO la leadership deve essere passata all'ERT, il quale farà in modo di svolgere le sue attività come da piano.

Definiamo delle misure di sicurezza da controllare quotidianamente.
1. Revisionare tutti i documenti importanti;
2. Salvare tutti i documenti elettronici in un network drive;
3. Mantenere un inventario accurato di tutti i beni materiali critici;
4. Fare del Cross-training ai dipendenti;
5. Assicurarsi che le Physical Security Procederus siano seguite;
6. Testare il funzionamento dei sistemy di backup/restore.

7. Testare il funzionamento dei sistemi di allarme;

5.2Attivazione del piano di contingenza

5.1.2 Definizione livelli di emergenza

Prima di definire gli eventi di attivazione del piano di contingenza è opportuno definire dei livelli di emergenza.

Livelli di Emergenza

Classe di emergenza	categoria	Impatto sull'organizzazione	Comunicazioni
I senza rilocamento	Alert	Un evento reale o previsto può avere un impatto negativo per meno di 12 ore con scarso effetto sui servizi o sulle funzioni essenziali. Non è richiesta l'attivazione del piano di emergenza, a seconda delle esigenze del singolo dipartimento	Il personale appropriato reagisce e risolve la situazione. I responsabili vengono contattati e resi consapevoli della situazione
II senza rilocamento	standby	Si stima che un evento reale o previsto abbia un impatto sulle operazioni per 12-72 ore, possibilmente richiedendo all'esterno. L'ERT determina se / quando è necessaria l'attivazione del piano di emergenza, in base ai requisiti delle singole aree.	Le aree interessate avvisano i responsabili della situazione e richiedono l'assistenza necessaria.

III con rilocamento	Attivazione limitata	Un evento reale interrompe minimamente le operazioni di una o più funzioni essenziali o influisce sui sistemi critici per un massimo di 7 giorni. Attivazione del piano di emergenza limitato. Potrebbe richiedere lo spostamento di alcuni membri del personale in un luogo di lavoro alternativo per meno di una settimana	Le aree interessate comunicano all'ERT la situazione, richiedono l'assistenza necessaria e possono inviare i dipendenti in luoghi di lavoro alternativi. L'ERT determina l'estensione dell'attivazione del CP.
IV con rilocamento	Attivazione completa	Un evento effettivamente interrompe in modo significativo le operazioni di tre o più funzioni essenziali o per l'intera organizzazione per più di una settimana, con la possibilità di durare fino a 30 giorni. Attivazione del piano di emergenza completo emessa dall'ERT.	Le aree interessate informano l'ERT della situazione, richiedono l'assistenza necessaria e inviano i dipendenti a un luogo di lavoro alternativo. I membri dell'ERT attivano il CP.

5.2.2 Eventi di attivazione del piano

Ricordiamo gli eventi che porterebbero all'attivazione del piano.

Evento	Livello di Emergenza
Alluvione	IV
Incendio	IV
Tornado	III
Tempeste elettriche	III
Terrorismo	III
Atti di sabotaggio	III
Danneggiamento Critico rete elettrica	IV
Danneggiamento Critico Intranet Aziendale/LAN	IV
Perdita di comunicazione tra network services	I
Mancanza di Fornitura dai Fornitori Esterni	II
Danneggiamento Computer	I
Perdita WI-Fi	II
Mancanza di dipendenti(influenze	I

stagionali,assenze non avvisate,scioperi)	
Danni alla sala server	III
Incidenti relativi al magazzino	II
Mancanza di supporto software per cause esterne	II
Danni al generatore elettrico/perdita di corrente elettrica	I
Scorretta update della base di dati	I

5.2.3 Punti di Evacuazione

Nel caso in cui sia necessario evacuare la strutture,il piano di contingenza indentifica due punti di evacuazione:

- primario-parcheggio dell'azienda;
- alternativo-parcheggio dell'azienda limitrofa;

5.2.4 Disaster Recovery Event Recording Form

- Tutti gli eventi chiave avvenuti durante la fase di disaster recovery vanno documentati
- Il disaster recovery team leader deve mantenere un log degli eventi
- Questo log degli eventi deve inziare all'inizio delle emergenze e una copia deve essere mantenuta anche dal business recovery team quando i primi incidenti sono stati controllati e chiusi.
- Il successivo event log deve essere completato dal disaster recovery team leader per segnare tutti gli eventi chiave avvenuti durante la disaster recovery fino a quel momento,poi la responsabilità viene data al business recovery team.

Descrizione dell'incidente:
Data di inizio:
Data/ora in cui è entrato in azione il DR team

Attività svolte dal DR Team	Data e ora	Risultato	Azione richiesta post risoluzione

Data di completamento del lavoro
Data del passaggio dell'event log al Business Recovery Team

5.2.5 Disaster Recovery Activity Report Form

- Dopo il completamento della prima risposta da parte del disaster recovery il DRT leader deve preparare un report sulle attività svolte.

- Questo report deve contenere tutte le informazioni sull’emergenza,chi è stato notificato e quando,tutte le azioni prese dai membri del DRT e tutti i risultati nati da queste azioni.
- Il report conterrà anche una stima sull’impatto alle normali operazioni di business.
- Una stima dell’efficienza del BCP
- Lezioni imparate

5.2.6 Emergency Alert ed Escalation

Questa policy e procedura è stata stabilita per garantire che nell’evento di un disastro/crisi,il personale abbia una chiara idea di chi debba essere contatato.
Le procedure sono state gestite in modo che le comunicazioni possano essere effettuate velocemente durante l’attivazione del disaster recovery.
Il piano di contingenza sarà dipendente da membri chiave dello staff/management i quali dovranno provvedere con le loro skill tecniche e manageriali alla veloce ed efficiente ripresa del business.
I fornitori di beni critici e servizi dovranno continuare a supportare la recovery delle operazioni di business durante il ritorno alla normalità.

Allerta di Emergenza

La persona che identifica l’incidente deve chiamare un membro dell’ERT nell’ordine riportato:

Emergency Response Team
- _____
- _____
- _____

Contatti alternativi:
- _____
- _____

L’emergency response team è responsabile dell’attivazione del Disaster Recovery Plan per gli eventi descritti in questo piano,inoltre deve anche occuparsi di qualsiasi altra occorrenza che inibisca la capacità di lavoro dell’azienda.

Una delle task avviate durante le prime fasi dell’emergenza è quella di notificare il Disaster Recovery Team dell’emergenza in avvenimento. La notifica richiederà ai membri del DRT di riunirsi al sito del problema e necessiterà di sufficienti informazioni per far sì che questa richiesta sia comunicata con efficacia.

Il Business Recovery Team sarà composto da rappresentati senior dai principali dipartimenti.
Il BRT leader dovrà essere un membro senior del management team dell’azienda,e sarà responsabile dell’outcome del processo di contingenza. Infine esso dovrà premurarsi che l’azienda torni a pieno regime il prima possibile.

Procedure di Disaster Recovery per il Management

I membri del management team dovranno tenere una hard coy dei nomi e numeri di contatto di ciascun impiegato nei loro dipartimenti di competenza. In aggiunta,i membri del management dovranno avere una hard copy dei file di Disaster Recovery e Continuity nelle loro case,nel caso in cui dovesse essere necessario consultarli e gli edifici dell’azienda fossero irraggiungibili o distrutti.

5.2.7 Contatto con i dipendenti

I manager serviranno da punto focale per i loro dipartimenti,mentre gli impiegati designati dovranno chiamare alti impiegati per discutere la crisi/disastro e i piani immediati per la compagnia. Gli impiegati che non riescono a contattare lo staff o la loro call list dovrebbero chiamare i numeri di telefono dei memebri dello staff emergenze,in modo da poter rifererire eventuali informazioni sul disastro.

Bisogna inoltre elencare le responsabilità del Team IT durante le operazioni di contingenza

1. identificare le funzioni che possono essere posticipate o cancellate temporaneamente,nel caso in cui si debba attivare il piano di contingenza;
2. Provvedere a dare informazioni,direzioni,obiettivi durante un'emergenza;
3. Amministrare gli sforzi di contingenza IT in tutte le locazioni;
4. Partecipare ai traning e test del piano di contingenza;
5. Assicurarsi di seguire le linee guida di alert notification;
6. Coordinare i propri sforzi con il personale amministrativo nel spostare il personale chiave nelle locazioni alternative di emergenza nel caso sia necessario un rilocamento;

Notifica dei familiari

Se l'incidente ha come risultato una situazione che potrebbe causare l'ospedalizzazione di un dipendente,dovrà essere imperativa la notifica dei suoi familiari.

Capitolo 6 Stabilimento di Contingency

Prima di definire i dettagli del cold/warm/hot standby ricordiamo sinteticamente i servizi chiave da mantenere e da cosa dipendono:

1. Gestione del ciclo di vita e della postazione di lavoro
   Questo servizio per poter essere svolto dipende dall'availability di:
   1. Personale Specializzato;
   2. Magazzino(per sostituzioni dell' hardware,consegna merci etc etc);
   3. Integrità dell'Ufficio/postazione di lavoro;
   4. Server;
   5. Dischi di aggiornamento software;
   6. Wi-Fi per download aggiornamenti;
   7. Librerie di backup;
   8. Intranet Aziendale/LAN;
   9. Computer,palmari e telefono;
   10. Backup site;
   11. Corrente Elettrica/reti Elettriche;
2. Manutenzione Hardware/Software
   Questo servizio per poter essere svolto dipende dall'availability di:
   1. Personale Specializzato;
   2. Integrità Ufficio;
   3. Wi-Fi

    4. Computer,palmari e telefono(su cui fare manutenzione);
    5. Corrente Elettrica/reti Elettriche;
3. Servizio di Help Desk I/II livello
   Questo servizio per poter essere svolto dipende dall'availability di:
    1. Personale Specializzato;
    2. Computer,Telefono;
    3. Intranet Aziendale/LAN;
    4. Elettricità/rete Elettrica;
    5. Integrità Ufficio;
    6. Integrità Call Center;
    7. Wi-Fi;
    8. Magazzino;
4. Servizio di "Monitoraggio " degli apparati di rete, delle linee dati
   Questo servizio per poter essere svolto dipende dall'availability di:
    1. Personale Specializzato;
    2. Intranet Aziendale/LAN;
    3. Wi-Fi;
    4. Server;
    5. Integrità Ufficio;
    6. Elettricità/Rete Elettrica;
    7. Software di Monitoraggio;
5. Servizio di "Ricezione Chiamate",Call Center Unico,Segreteria Aziendale
   Questo servizio per poter essere svolto dipende dall'availability di:
    1. Personale Specializzato;
    2. Intranet Aziendale/LAN;
    3. Wi-Fi;
    4. Integrità Ufficio;
    5. Integrità Ufficio segreteria;
    6. Integrità Call Center;
    7. Elettricità/Rete Elettrica;
    8. Integrità Rete Telefonica;
    9. Integrità Attrezzatura Medica;
6. Servizi ITIL(incident management etc etc) + Remote Desktop Controls
   Questo servizio per poter essere svolto dipende dall'availability di:
    1. Personale Specializzato;
    2. Intranet Aziendale/LAN;
    3. Wi-Fi;
    4. Integrità Ufficio sezione IT;
    5. Integrità Uffficio sezione Area Medica;
    6. Elettricità/Rete Elettrica ;
    7. Integrità Call Center;
    8. Integrità Rete Telefonica;

6.1 Interni
6.1.1 Cold Standby

Consiste di una facility dotata di adeguato spazio e infrastrutture (energia elettrica,telecomunicazione e clima) per fare da supporto ai sistemi IT.
Lo spazio può anche essere dotato di piani rialzati e altre caratteristiche utili alle operazioni IT.
Il site non conterrà strumentazione lavorativa,ad esempio telefoni,stampanti etc.
Questa strumentazione sarà da trasportare dal magazzino nel caso di bisogno.
Può essere usata quando un business può funzionare fino a 72 ore circa senza bisogno dei servizi IT

Nel caso di questo piano di Contingenza una stanza di cold standby è d'obbligo,nel caso che un ufficio sia compromesso (alluvione,incendio….)una stanza vuota in cui trasportare i computer per continuare il lavoro risolve molti problemi.

Il personale attivo dovrà quindi usufruire temporaneamente della stanza in cold standby,dotata di:

1. Collegamenti alla Intranet Aziendale/LAN autonomi;
2. Wi-Fi autonomo;
3. Situata al secondo piano dell'edificio principale(o comunque ad un piano diverso dagli uffici,per essere isolata da alluvioni);
4. Rete Elettrica collegata al generatore autonomo d'emergenza;
5. Copie della Documentazione D'emergenza(esempio:copia di questo documento).

La strumentazione del Cold Site non farà uso del sistema di Mirror Backup,avrà quindi solo computer da rendere operativi in giornata.

Il Cold Site verrà utilizzato per gli incidenti di classe I e II,sarà quindi usato per gli incidenti dove non è necessario il rilocamento del personale.

I servizi che potrebbero essere destabilizzati dagli incidenti di classe I e II sono:
1. Gestione ciclo di vita postazione di lavoro;
2. Manutenzione Hardware/Software;
3. Servizio Help desk;
4. Servizi ITIL(incident management etc etc) + Remote Desktop Controls

6.1.2 Warm Standby

Solitamente coinvolge il ripristino dei sistemi critici e dei servizi entro un periodo di 24 ore circa. Può essere interna od esterna, fissa o portatile, e consiste di una struttura informativa contenente delle attrezzature di ripristino IT che possono essere configurate per supportare il business

Il Warm Site avrà un mirroring asincrono,non sarà quindi aggiornato passo passo con i server principali e sarà utilizzato assieme al cold site per incidenti di classe I e II.

Nei casi in cui gli incidenti di questo livello dovessero richiedere spazi più ampi il warm site darà a disposizione dati al cold site per velocizzare il processo di ritorno alla normalità.
Nel caso in cui il solo cold site o il solo warm site non siano in grado di risolvere l'incidente,i due spazi dovranno collaborare.
Il cold site offrirà il suo più ingente spazio (dato che è vuoto può permettersi una metratura più ampia) e il warm site i suoi dati con mirroring asincrono.
In questo modo si potrà risolvere un ampio spettro di incidenti mettendo assieme i punti di forza del cold site e del warm site,oppure se necessario usare solo uno o solo l'altro.

Il warm site sarà quindi quello più utilizzato nella quotidianità,per piccoli restore di dati ad hoc.

6.2 Esterni

Prima di stabilire l'hot site,facciamo il punto di quali sono i criteri da considerare:

1. Area Geografica:ovvero la distanza dall'edificio aziendale e la probabilità che l'hot site sia danneggiato dallo stesso incidente avvenuto nell'edificio principale;
2. Accessibilità:è necessario tenere in considerazione il tempo speso per accedere all'hot site;
3. Sicurezza:norme di sicurezza adottate e fiducia negli impiegati che ci operano,queste devono essere a livello con la confidenzialità dei dati in questione;
4. Costo:il quale non sarà descritto in questo piano di contingenza.

6.2.1 Hot Standby

Prevede l'impiego di stabilimenti alternativi con un continuo mirroring dell'ambiente live, inclusi i dati
Può essere interna od esterna ed è l'opzione più costosa
Dovrebbe essere usata solo per quei servizi più critici per il business, la cui perdita comporterebbe un impatto immediato per il business

Nel caso di questo piano di contingenza l'uso di un Hot site è fondamentale,a differenza del cold/warm standby,l'hot site avrà una stanza completamente indipendente dall'edificio principale.

Verrà utilizzato per gli incidenti di livello III e IV

5. Alluvione del primo piano;
6. Incendio;
7. Perdita Corrente elettrica che duri più di un ora;
8. Perdita del Wi-Fi;
9. Danneggiamento alla Intranet Aziendale/Lan;
10. Danneggiamento in generale di più di un Computer;
11. Sabotaggio;
12. Tempeste Elettriche;

L'hot site avrà le seguenti caratteristiche:

2. Sala Server di backup;
3. Librerie di Backup;

4. Magazzino Secondario (anche più piccolo del primario ma contenente le apparecchiature di ricambio più utilizzate);
5. Computer di backup,pronti all'uso;
6. Fully mirrored site;
7. Sarà posto in un edificio esterno all'ufficio principale;
8. Sarà posto ad un piano elevato(per risolvere il problema alluvione);
9. Metratura abbastanza ampia per permettere a diversi dipendenti di lavorarci;

L'hot site sarà utilizzato per il rilocamento del personale,nel caso in cui gli incidenti sono di un livello tale da rendere inutilizzabile l'edificio principale.
Il sito dovrà essere monitorato e aggiornato quotidianamente.
L'hot site verrà utilizzato per il recover di questi servizi:

- Servizio di "Monitoraggio " degli apparati di rete, delle linee dati
- Servizio di "Ricezione Chiamate",Call Center Unico,Segreteria Aziendale
- Servizi ITIL(incident management etc etc) + Remote Desktop Controls

Riepilogo sulle strategie di Equipment Replacement

Nel caso in cui servano dei ricambi al sistema IT o in cui l'edificio principale non sia accessbile,l'hardware e software necessari dovranno essere trasportati velocemente in una locazione alternativa.
In questo caso questa locazione può essere il cold site (se l'edificio principale è operativo) o l'hot site (se l'edificio principale non è operativo).
Per fare ciò utilizziamo 3 strategie diverse,da implementare in casi specifici a seconda delle necessità:

1. Vendor Agreements:con l'avanzare del piano di contingenza,si posso fare SLA di hardware,software e fornitori per il mantenimento d'emergenza del servizio. Gli SLA dovranno specificare quanto velocemente debba rispondere il fornitore dopo esser stato notificato. L'accordo deve anche dare all'organizzazione uno status prioritario per la spedizione dell'equipaggiamento di ricambio. Lo SLA deve anche discutere quale livello di priorità dovrà ricevere nel caso di eventi catastrofici,relativamente ai livelli di priorità delle altre organizzazioni. Nel nostro caso, la nostra organizzazione dovrà avere priorità massima, visto che opera a supporto di una Azienda Sanitaria;
2. Equipment inventory:l'equipaggiamento richiesto sarà comprato in anticipo e posto nel magazzino(oppure nel warm o hot site a seconda delle necessità);
3. Existing Compatible Equipment:l'equipaggiamento già magazzinato o usato nell'hot site può già essere usato in caso di emergenza,questo avverrebbe in casi estremi in cui nel magazzino o dal fornitore non sia presente un certo equipaggiamento e sia necessario usarne uno subito. Dopo averlo usato come ricambio dovrà esserne comprata un altra unità non appena disponibile,da essere immagazzinata come equipment inventory.

Capitolo 7 Procedure operative

Questa sezione descrive le procedure per il recover delle operazioni in un sito alternativo,mentre altri sforzi sono diretti a riparare i danni al sistema e alle capacità originali.

Le procedure dovranno essere assegnate al DRT formato dall'ERT e seguiranno le seguenti azioni:

1. ottenere autorizzazione ad accedere agli edifici incidentati;
2. notificare i business partner interni/esterni relativi al sistema;
3. ottenere la strumentazione e spazio di lavoro necessari;
4. ottenere ed installare i necessari componenti hardware;
5. ottenere ed installare i media di backup;
6. ristabilire i sistemi operativi critici e le applicazioni software;
7. ristabilire i dati di sistema;
8. testare il funzionamento del sistema,inclusi i protocolli di sicurezza;
9. connettere il sistema al network o ad altri sistemi esterni;
10. utilizzare l'equipaggiamento alternativo con successo;

Andiamo ora a descrivere le procedure operative per per il rilocamento di alcuni servizi chiave

7.1 Cold standby

La sala di cold standby deve essere utilizzata come rilocamento del personale nel caso in cui gli uffici non siano utilizzabili. Scelto dall'ERT,l'alternate site relocation team farà da management alle operazioni.

Le procedure per il recovering del Servizio di Help Desk I/II nel sito alternativo dovranno essere eseguite nell'ordine seguente:

Recovery Goal 1:Approntare il Cold Site come Help Desk alternativo:
Team assegnato: Transportation and Relocation Team
Nel minore tempo possibile questo team deve trasportare i computer e telefoni necessari nella sala

Recovery Goal 2:Configurare la strumentazione
Team assegnato:Application Recovery Team
I dati e software necessari dovranno essere recuperati usando i backup del warm/hot site,a seconda del caso.

Recovery Goal 3:Testing
Team assegnato:Application Recovery Team
Dopo l'avvenuta configuraziobe delle strumentazione sarà dovuto un veloce test dell'effetivo funzionamento della stessa

Recovery Goal 4: Notifica

Team assegnato:Alternate site relocation team
Avvenuta la configurazione e riscontratone il funzionamento è infine necessario avvisare del successo del rilocamento,in modo da poter iniziare le procedure lavorative.

Questa procedura è la procedura standard da utilizzare per garantire un uso efficace del cold site,può essere utilizzata anche nel recover di altri servizi,oltre al servizio di help desk.

7.2 Warm standby

La sala di warm standby non offre molto spazio per il rilocamento del personale,essa deve essere usata come sala di backup delle informazioni di media importanza(dato che usa mirroring asincrono).
Le procedure operative risultano quindi molto semplici, si tratta di regolare lo spostamento di dati dal warm site al resto del dipartimento, per fare ciò è sufficiente seguire le linee guida illustrate in precedenza.

Recovery Goal 1:Permessi
Team assegnato:Transportation and Relocation Team
Per poter trasportare materiali dal warm site a dove sono richiesti, per prima cosa bisogna ottenere il “permesso” secondo le eventuali regole di confidenzialità nel caso di documenti ad alto livello di riservatezza ad esempio. Il management del team deve quindi avvisare il gestore dell’inventario del warm site.

Recobery goal 2:Documentazione
Team assegnato:Warm site manager
Il manager del warm site deve quindi prendere nota dei materiali che sono stati rilocati ed accertarsi che alla fine delle operazioni di recovery questi ritornino al loro posto,per fare ciò deve tenere un log entrata/uscita dei materiali magazzinati nel warm site

7.3 Hot standby

La sala di hot standby è situata in un edificio diverso da quello principale,deve essere usata con rilocamento da un team di media grandezza nel caso in cui tutto l’edificio principale non sia accedibile.

Le procedure per il recovering del Servizio di “Monitoraggio “ degli apparati di rete e delle linee dati nel sito alternativo dovranno essere eseguite nell’ordine seguente:

Recovery Goal 1: Rilocamento del personale necessario
Team assegnato: alternate site relocation team
L’hot site disponde di una modesta metratura,quindi è necessario operare un rilocamento selezionando il personale chiave.

Bisogna precisare che l’uso dell’hot site con rilocamento avviene quando l’intero edificio principale non è raggiungibile,ciò implica l’avvenimento di un incidente di alto livello,quindi è molto probabile di non poter disporre di tutto l’organico. Anche questa informazione contribuisce al voler rilocare il minor numero di dipendenti possibile.

Recovery goal 2:Testing
Team assegnato:Test Team
Anche se l’hot site viene periodicamente controllato,è necessario fare un test della corretta funzionalità dei sistemi,prima di iniziare ad utilizzarli;

Recovery Goal 3:Verificare di avere tutta la strumentazione necessaria
Team assegnati:Test Team
L’hot site dispone di un piccolo magazzino contenente la strumentazione chiave,ma la sua capacità è molto più ristretta rispetto al magazzino principale. Nel caso in cui uno strumento non sia presente bisogna coordinarsi con l’ERT per verificare la possibilità di reperire lo strumento nel magazzino principale.

Recovery Goal 4:Verificare la funzionalità del network
Team assegnati:Test Team
Nel caso in cui LAN/WAN/connessione internet non funzionino,il test team deve contattare il LAN/WAN Recovery Team o il Telecommunications Team. Questi dovranno utlizzare le strategie di contingenza descritte nei capitoli precedenti per assicurare all’hot site il corretto funzionamento.

Recovery goal 5: riprendere il lavoro
Team assegnati: Team scelto dall’ERT
Questo goal è ovvio,il personale scelto dopo aver appurato che tutto funzioni deve mettersi al lavoro sul servizio di monitoraggio.

Le procedure per il recovering del Servizio di “Ricezione Chiamate”,Call Center Unico,Segreteria Aziendale degli apparati di rete e delle linee dati nel sito alternativo dovranno essere eseguite nell’ordine seguente:

Recovery Goal 1: Rilocamento del personale necessario
Team assegnato: alternate site relocation team
L’hot site disponde di una modesta metratura,quindi è necessario operare un rilocamento selezionando il personale chiave. In questo caso saranno necessari membri esperti dell’originale servizio di segreteria Aziendale,affiancati da esperti dell’infrastruttura IT dell’hot site,in modo da poter avere un campo di expertise ampio nel caso in cui si presentino problemi con l’attrezzatura.

Recovery goal 2:Testing
Team assegnato:Test Team
Anche se l’hot site viene periodicamente controllato,è necessario fare un test della corretta funzionalità dei sistemi,prima di iniziare ad utilizzarli;

Recovery Goal 3:Verificare la funzionalità del network
Team assegnati:Test Team
Nel caso in cui LAN/WAN/connessione internet non funzionino,il test team deve contattare il LAN/WAN Recovery Team o il Telecommunications Team. Questi dovranno utlizzare le strategie di contingenza descritte nei capitoli precedenti per assicurare all'hot site il corretto funzionamento.

Recovery goal 4:Notifica
Team assegnato:Administrative Support Team
Dopo il test è necessario avvisare tutti i contatti di lavoro/clienti del temporaneo rilocamento della segreteria aziendale,ciò è importante per vari motivi:

1. il numero telefonico della segreteria potrebbe essere cambiato;
2. se la segreteria utilizzava un banco d'assistenza fisico,bisogna avvisare del suo rilocamento e di eventuali variazioni di orario;
3. il personale potrebbe risultare ridotto rispetto a prima,questo va notificato poiché riduce la capacità lavorativa del team;

Recovery Goal 5:Verificare di avere tutta la strumentazione necessaria
Team assegnati:Test Team
L'hot site dispone di un piccolo magazzino contenente la strumentazione chiave,ma la sua capacità è molto più ristretta rispetto al magazzino principale. Nel caso in cui uno strumento non sia presente bisogna coordinarsi con l'ERT per verificare la possibilità di reperire lo strumento nel magazzino principale.

Recovery goal 6: riprendere il lavoro
Team assegnati: Team scelto dall'ERT
Questo goal è ovvio,il personale scelto dopo aver appurato che tutto funzioni deve mettersi al lavoro sul servizio di monitoraggio.

Capitolo 8 Sicurezza

Le funzioni di protezione dai virus informatici sui client e sui server sono assicurate mediante la NeatSuite di Trend Micro. La suite comprende InterScan Messaging™ Security Suite, ed InterScan™ Web Security Suite, ScanMail™ for Microsoft™ Exchange con eManager, e ServerProtect™ per Microsoft Windows per sevres di classe enterprise ed OfficeScan™ per desktop e server.

Le soluzioni di contingenza che saranno descritte dovrebbero essere operate coordinandosi con le policy di sicurezza e i controlli di sicurezza. In modo che durante un interruzione di sistema o un incidente non vengano divulgati dati sensibili.

Per aumentare l'integrità del nostro sistema aziendale,dato l'alto uso di firme digitale ed encryption per la confidenzialità,è necessario utilizzare delle coppie di encription keys.
Inoltre nel caso di computer portatili e palmari,l'encryption è necessaria per proteggere i dati in caso di furto.
Se le encription keys e la chiave di verifica sono salvate direttamente nel PC,i dati possono diventare irrecuperabili nell'eventualità che il PC diventi corrotto.

I dipendenti dotati di computer portatile dovrebbero anche essere forniti di un secondo hard drive,da usare in viaggio. Questo secondo hard drive conterrà solo le minime informazioni e applicazioni necessario. Così facendo in caso di perdita o furto del laptop,la quantità di dati persa sarà minimizzata.

8.1 Availability

Per mantenere una il più possibile alta availability,oltre alle soluzioni già illustrate negli scorsi capitoli,si è deciso di implementare anche queste strategie:

1. alimentatori non interrompibili della grandezza giusta per garantire dell'energia di backup momentanea per tutti i system components;
2. Generatore principale e di backup a gasolio/diesel per garantire energia a lungo termine;
3. Sistemi di areazione con abbastanza capacità eccedente per permettere la failure di alcune componenti,ad esempio compressori;
4. Sistemi di soppressione incendi;
5. Rilevatori di fumo;
6. Sensori posti nel soffitto e pavimento delle sale server/computer atti a rilevare ristagni d'acqua;
7. Teli di plastica atti a venir predisposti per proteggere dispositivi IT da danni causati dall'acqua;
8. Contenitori resistenti ad alte temperature e all'acqua per media di backup;
9. Master system shutdown switch d'emergenza;
10. Controlli di sicurezza,management delle chiavi crittografiche e accesso privilegiato;

8.2Confidentiality

Le strategie utilizzate per mantenere la confidenzialità dei dati oltre a quelle già descritte nei capitoli precedenti,sono:

1. Crittografare i file critici,questo processo rende i dati illeggibili a chiunque non possegga la chiave o password giusta. Queste saranno gestite dall'head of security;
2. Controllare l'accesso ai dati,è necessario stilare una access list periodica per definire chi può accedere a quali file. Questa lista deve essere revisionata periodicamente rimuovendo o aggiungendo membri in base alle necessità;
3. Mantenere fisicamente sicuri i device e i documenti cartacei,non solo i dati ma anche tutti gli altri tipi di dati contenuti nella media library devono essere messi in sicurezza. Per fare ciò è necessario rendere la stanza della definitive media library un luogo ad accesso limitato, definendo quindi un manager della stessa, i quale sarà deciso dall'head of security;
4. Distruzione sicura di dati,devices e documenti cartacei, qualsiasi dato sensibile ospedaliero non più utile deve essere smaltito con cura,in modo che sia irrecuperabile. I documenti cartacei devono essere triturati piuttosto che gettati via interi e i dati sensibili devono essere cancellati in sicurezza,in modo che non possano più essere recuperati;
5. Privacy e confidenzialità,i dati ospedalieri dei pazienti devono essere acquisiti con discrezione e nella totale aderenza alle leggi sulla privacy;
6. Buon management dei dati sensibili,l'uso della label "sensitive data" deve essere utilizzata solo nei casi in cui c'è un effettivo bisogno di essa;
7. Management dei device:
    1. Patch ricorrenti del software;
    2. Anti-virus;
    3. cambio frequente delle password personali;
    4. sospendere le sessioni inattive;
    5. usare firewall;
    6. usare crittografia del disco;

8.3 Integrity

Un altra soluzione di contingenza che sarà utilizzata è quella dell'imaging.
Una immagine standard del PC può essere salvata per poi essere utilizzata in un computer corrotto.
L'imaging installerà le applicazioni necessarie e i setting salvati nell'immagine,però così facendo tutti i dati del disco andranno persi.
Per far fronte a ciò,tutti i dipendenti dovranno essere incoraggiati a fare backup dei loro dati.
Dato il fatto che le immagini dei dischi potrebbero essere di grande quantità,saranno allocate in una partizione del server.
Per decrescere il numero di immagini necessarie per la recovery nell'evento che molti PC diventino corrotto, sarà necessario standardizzare i modelli e le configurazione dei PC in tutta l'azienda.
Facendo così si salverà spazi e velocizzerà il processo di ritorno alla normalità.

Un altra minaccia all'integrità dei PC è l'avvenuta corruzione di un computer a fronte di una caduta di corrente. Per far fronte a ciò si possono configurare i PC con la capacità di poter utilizzare un sistema a dual power supply. La configurazione a doppia alimentazione farà in modo che le due alimentazioni lavorino simultaneamente,così che se l'alimentazione principale dovesse fallire,la seconda unità proteggerà l'hardware,ma non risolverà il problema della caduta elettrica.
Per risolvere questo problema è necessario un UPS,il quale garantirà dai 30 a 60 minuti di energia elettrica per finire i backup e spegnere i sistemi.
Questo sistema deve essere utilizzati in tutti i server aziendali,mentre non è strettamente necessario per i singoli pc,dato che i loro dati possono essere recuperati tramite le modalità già descritte nei capitoli scorsi.

Capitolo 9 Ritorno alla normalità

Nella fasi di ritorno alla normalità,le attività di recupero sono terminate e le operazioni lavorative sono ritrasferite agli uffici.
Nel caso in cui l'edificio principale non sia recuperabile,le attività descritte in questa fase sono applicabili anche alla preparazione di un nuovo sito operativo. Dopo aver recuperato il sito di backup o quello originale,ad un livello tale da permettere il normale svolgimento dei servizi e supportare il sistema IT, il sistema potrà essere riallocato nel sito di backup o quello originale.

Finché il sistema primario viene recuperato e testato,il sistema di contingenza deve continuare le sue mansioni.

L'ERT deve specificare i membri del DRT responsabili per il recupero sia del sito che del sistema IT, formando gli Alternate Site Recovery Coordination Team e Original Site Restoration/Salvage Coordination Team.
Mentre per il rilocamento del personale e delle risorse il compito sarà dato al transportation and relocation Team.

In questa fase dovranno essere svolte le seguenti attività:

1. Assicurare adeguato supporto infrastrutturale,come energia elettrica,acqua,telecomunicazioni,sicurezza,controlli ambientali,oggetti da ufficio e strumentazione generica;
2. installare hardware,software e firmware. Questa attività deve includere dettagliate procedura di recupero simili a quelle descritte nella fase di recupero;
3. stabilire connettività e interfacce con le componenti network e con i sistemi esterni;
4. Fare testing dei sistemi per assicurarne il pieno funzionamento;
5. Arrestare i sistemi di contingenza;
6. Terminare le operazioni di contingenza;
7. mettere in sicurezza,rimuovere e/o ricollocare tutto il materiali sensibile dal sito di contingenza;
8. Fare in modo che il personale di recovery posso tornare alle mansioni quotidiane. I team di contingenza dovranno essere abbastanza competenti da poter svolgere le loro funzioni senza dover seguire un piano cartaceo,nell'eventualità che questo non sia disponibile;

I processi di RAN devono essere svolti in concorrenza tra il sito originale e il nuovo. In questo modo il trasferimento delle operazioni lavorative da un sito all'altro potrà avvenire con maggiore fluidità ed efficienza

Infine durante la fase di de-attivazione del piano,il sito alternativo dovrà essere ripulito di qualsiasi equipaggiamento che non fosse definito standard per il sito. I materiali,media di backup dovranno essere impacchettati in modo appropriato e rilocati nel proprio posto assegnato. Durante questa fase dovranno essere seguite le linee guida descritte nel capitolo di availability,integrity e security.
Concluse queste operazioni,i team del DRT assegnati dall'ERT dovranno tornare ai propri lavori quotidiani.

9.1 Procedura di RAN per il cold site

RAN goal 1 Test di validazione dei dati
Team assegnato: Test team
I dati del cold site per prima cosa dovranno essere testati,in modo da assicurare la completa recovery dei file di dati o database al main site.

RAN goal 2 Test di validazione delle funzionalità
Team assegnato: Test team
La corretta funzionalità di tutti i sistemi dovrà essere testata, in modo da garantire il loro corretto uso nel ritorno alle normali operazioni.

RAN goal 3 Dichiarazione di recovery
Team assegnato:Test team
Dopo aver completato con successo le fasi di validation testing e functional validation testing, il risultato dovrà essere dichiarato e trasmesso al Original Site Restoration Coordination Team.

RAN goal 4 Notifica
Team assegnato:Administrative Support Team
Dopo la dichiarazione di recovery, gli user e i clienti devono essere notificati.
Questa operazione deve essere svolta seguendo le linee guida descritte nel capitolo sul personale.

RAN goal 5 Pulizia
Team assegnato: alternate site relocation team
Dato che tutta la strumentazione usata nel cold site è stata trasportata lì(come descritto nei capitoli precedenti) tutta la strumentazione deve essere portata via. Gli strumenti dovranno essere ricollocati negli ambienti nei quali si trovavano, dopo aver appurato il loro effettivo funzionamento.

RAN goal 6 Restituire il Backup Media
Team assegnato: alternate site relocation team
I media di backup e di installazione usati durante le operazioni di recovery devono essere riportati nel loro luogo d’origine,secondo le direttive specificate nei capitoli scorsi.

RAN goal 7 Fare backup dei sistemi
Il prima possibile dopo il recovery, bisogna fare un backup completo
Non appena ragionevole dopo il ripristino, è necessario eseguire il backup completo del sistema e archiviare una nuova copia dell'attuale sistema operativo per futuri sforzi di recupero. Questo backup completo viene quindi conservato con altri backup del sistema.

RAN goal 8 Documentazione degli eventi
Team assegnato: Original Site Restoration Coordination Team
è di vitale importanza mantenere un diario degli eventi, adattando il template fornito nel capitolo 2.1 di questo testo.

9.2 Procedura di RAN per il Warm Site

Come spiegato nel capitolo dedicatogli,il warm site non offre spazio per il rilocamento del personale,ma funge come backup asincrono in supporto al cold site.
Quindi le uniche operazioni che si possono eseguire sono quelle di rilocamento dei dati dal warm al cold site.

RAN goal 1 Inventario
Team assegnato:Manager Warm Site
La strumentazione rilocata durante le procedure di recovery è stata riportata nel warm site, adesso il manager deve controllare dalla documentazione la presenza di tutto il materiale usato ed il suo corretto funzionamento.

9.3 Procedura di RAN per l'hot site

L'hot site si trova in un edificio diverso da quello principale,quindi la procedura resta simile a quella del cold site ma con qualche differenza,specialmente nel trattamento della strumentazione.

RAN goal 1 Test di validazione dei dati
Team assegnato: Test team
I dati del warm site per prima cosa dovranno essere testati,in modo da assicurare la completa recovery dei file di dati o database al main site.

RAN goal 2 Test di validazione delle funzionalità
Team assegnato: Test team
La corretta funzionalità di tutti i sistemi dovrà essere testata, in modo da garantire il loro corretto uso nel ritorno alle normali operazioni.

RAN goal 3 Dichiarazione di recovery
Team assegnato:Test team
Dopo aver completato con successo le fasi di validation testing e functional validation testing, il risultato dovrà essere dichiarato e trasmesso al Original Site Restoration Coordination Team.

RAN goal 4 Notifica
Team assegnato:Administrative Support Team
Dopo la dichiarazione di recovery, gli user e i clienti devono essere notificati.
Questa operazione deve essere svolta seguendo le linee guida descritte nel capitolo sul personale.

RAN goal 5 Pulizia
Team assegnato: alternate site relocation team
L'hot site da piano di contingenza è già fornito di equipaggiamento di backup,quindi durante la fase di pulizia è necessario individuare la strumentazione che deve restare nell'hot site e quella che invece è stata portata durante le operazioni di recovery.

RAN goal 6 Restituire il Backup Media
Team assegnato: alternate site relocation team

I media di backup e di installazione usati durante le operazioni di recovery devono essere riportati nel loro luogo d’origine,secondo le direttive specificate nei capitoli scorsi.

RAN goal 7 Fare backup dei sistemi
Team assegnato:Original Site Restoration Team
Il prima possibile dopo il recovery, bisogna fare un backup completo
Non appena ragionevole dopo il ripristino, è necessario eseguire il backup completo del sistema e archiviare una nuova copia dell'attuale sistema operativo per futuri sforzi di recupero. Questo backup completo viene quindi conservato con altri backup del sistema.

RAN goal 8 Documentazione degli eventi
Team assegnato: Original Site Restoration Coordination Team
è di vitale importanza mantenere un diario degli eventi, adattando il template fornito nel capitolo 2.1 di questo testo.

Allegato: Elenco delle attrezzature informatiche aziendali

Elenco dei Computer aziendali

		Quantità
ACER	ASPIRE 1350	1
ACER	EXTENSA 5620	3
ACER	TRAVEL MATE C200	1
ACER	TRAVELMATE 261XC	1
ACER	TRAVELMATE 2700	9
ACER	TRAVELMATE 3000	2
ACER	TRAVELMATE 4060	39
ACER	TRAVELMATE 4150	1
ACER	TRAVELMATE 4650	4
ACER	TRAVELMATE 522TX	1
ACER	TRAVELMATE 6410	4
ACER	TRAVELMATE 739TLV	1
ACER	TRAVELMATE 8100	8
ACER	TRAVELMATE C102TI	1
ACER	TRAVELMATE C200	4
ACER	TRAVELMATE3000	1
ACER	TRAVELMATE6410	1
ASSEMBLATO	ASSEMBLATO	1
AST	BRAVO MS P/100	1
ASUS	A2500H	3
ASUS	A2550H NOTEBOOKPC	1
COMPAQ	DESKPRO	5
DATAMATIC	WELCOME	2
DELL	OPTIPLEX	1
ELETTRODATA	SAMARA S519+	1
ERGO	STA683	2
FLYBOOH	V33I	1
FUJITSU SIEMENS	AMILO PRO	11
FUJITSU SIEMENS	C-1020	1
FUJITSU SIEMENS	CELSIUS M430	1
FUJITSU SIEMENS	LIFEBOOK	1
FUJITSU SIEMENS	LIFEBOOK C 1020	1
FUJITSU SIEMENS	LIFEBOOK C SERIES	7
FUJITSU SIEMENS	LIFEBOOK E SERIES	4
FUJITSU SIEMENS	LIFEBOOK E4010	1
FUJITSU SIEMENS	M12W-D1521	3
FUJITSU SIEMENS	SCENIC	5
FUJITSU SIEMENS	SCENIC E600	9
FUJITSU SIEMENS	SCENIC MI2W-01521	1
FUJITSU SIEMENS	SCENIC P300	257
FUJITSU SIEMENS	SCENIC T	152
FUJITSU SIEMENS	SCENIC W600	12
GHIBLI	GHIBLI 10	4
GHIBLI	MT11	1
GOODNAME	PC CLONE	1
HIGHSCREEN	PC CLONE	1
HP	1740	1

HP	COMPAQ	1
HP	COMPAQ 6710B	1
HP	COMPAQ DC 1700 CMT	1
HP	COMPAQ1700CMT	1
HP	D330 DT	4

HP	D530 CMT	268
HP	D539 CMT BASE MODEL	2
HP	DC6100 CMT	2
HP	DC700	1
HP	DC7100 CMT	430
HP	DC7600 CMT	141
HP	DC7700 CMT	216
HP	DC7800 CMT	112
HP	HP COMPAQ	1
HP	HUB43900NF	1
HP	HUB4410GFC	1
HP	OMNIBOOK 6000	1
HP	OMNIBOOK XE3	2
HP	P7586T	1
HP	PAVILLION ZX5000	1
HP	P-M760	1
HP	VECTRA	1
IBM	PERSONAL COMPUTER 300GL	3
INTERCOMP	DT9	4
INTERCOMP	I20598	1
INTERCOMP	MASTER	3
INTERCOMP	MT11	20
INTERCOMP	MT12	4
INTERCOMP	MT9	1
INTERCOMP	OMADA	2
INTERCOMP	TS30T	1
MEGABYTE	ENTRY	1
MICRONICA/CDC	NON INDICATO	1
MITAS	PC CLONE	2
OEM CELERON	MT11	4
OLIDATA	DENVER	65
OLIVETTI	M24 XS	1
OMEGAPC	PIII	1
PC CLONE	PC CLONE	6
SAM@RA	S519+	1
SI COMPUTER	ACTIVA	50
SONY	VAIO PCG-4L2M	1
SONY	VAIO VGN-SZ3XP/C	1
TATUNG	TTABA12D	1
TATUNG COMPANY	TABLETPC	1
TOSHIBA	SATELLITE	1
VIBIS	EVXA	1
VOBIS	HIGHSCREEN R.T.R.	1
VOBIS	PC CLONE	1
ZENITH DATA SYSTEMS	POWERMATE ES	5
ZENITH DATA SYSTEMS	POWERMATE VT	11
ZENITH DATA SYSTEMS	Z STATION EL	1
ZENITH DATA SYSTEMS	Z STATION ES/P	1
ZENITH DATA SYSTEMS	Z-STATION 3100 E	4
ZENITH DATA SYSTEMS	Z-STATION EL	5

ZENITH DATA SYSTEMS	Z-STATION ES/P	2
	Totale	**1972**

Elenco delle Stampanti aziendali

BROTHER		1
BROTHER	HL-1240	8
BROTHER	HL-1250	11
BROTHER	HL-1440	31
BROTHER	HL-1450	28
BROTHER	HL-2060	1
BROTHER	HL-5050	271
BROTHER	HL-5140	6
BROTHER	HL-5150D	16
BROTHER	HL-550	1
BROTHER	HL-8080	1
BROTHER	HL-P2500	2
BROTHER	QL-550	1
BULL	COMPUPRINT 4/54	2
BULL	COMPUPRINT 4056	2
BULL	COMPUPRINT 970	1
BULL	COMPUPRINT SIGNUM 2048	1
BULL	PAGEPRO 1100L	28
BULL	SIGNUM 2048	1
CANON	BJC-3000	3
CANON	BJC-50	1
EPSON	C60	1
EPSON	COLOR 760	1
EPSON	DFX-8500	2
EPSON	EASYCODER C4	1
EPSON	EPL-5600	1
EPSON	EPL-5700	1
EPSON	ESTYLUS COLOR850	1
EPSON	LQ-2090	2
EPSON	LQ-300+	1
EPSON	LQ-680	14
EPSON	LQL680	1
EPSON	LX 850	1
EPSON	STYLUS C60	1
EPSON	STYLUS C64	1
EPSON	STYLUS C84	2
EPSON	STYLUS COLOR 1160	1
EPSON	STYLUS COLOR 400	17
EPSON	STYLUS COLOR 440	3
EPSON	STYLUS COLOR 600	1
EPSON	STYLUS COLOR 660	4
EPSON	STYLUS COLOR 760	1
EPSON	STYLUS COLOR 800	2
EPSON	STYLUS COLOR 850	9
EPSON	STYLUS COLOR 880	1
EPSON	STYLUS PHOTO 1290	1
EPSON	STYLUS PHOTO 750	1

EPSON	STYLUS PHOTO 810	1
HP	COLOR LASERJET	1
HP	COLOR LASERJET 3700	37
HP	COLOR LASERJET 4700	1
HP	COLOR LASERJET CP3505	1

HP	COLOR LASERJET4700N	1
HP	DESIGNJET 70	1
HP	DESINGET 500 (SCANNER)	1
HP	DESKJET 1120C	1
HP	DESKJET 1220C	1
HP	DESKJET 3420	3
HP	DESKJET 3820	1
HP	DESKJET 5652	4
HP	DESKJET 600	2
HP	DESKJET 6122	1
HP	DESKJET 640C	1
HP	DESKJET 656C	1
HP	DESKJET 660C	1
HP	DESKJET 695	1
HP	DESKJET 710C	3
HP	DESKJET 840C	16
HP	DESKJET 902C	1
HP	DESKJET 920C	1
HP	DESKJET 930C	4
HP	DESKJET 940C	11
HP	DESKJET 960C	2
HP	DESKJET 980CXI	1
HP	DESKJET F380	1
HP	DESKJET5652	1
HP	DESKJET940C	1
HP	EASYCODER C4	1
HP	LASERJET	2
HP	LASERJET 1005	1
HP	LASERJET 1100	1
HP	LASERJET 1200 SERIES	1
HP	LASERJET 1300	2
HP	LASERJET 2300	101
hp	LASERJET 2420	520
HP	LASERJET 2440	3
HP	LASERJET 2500	5
HP	LASERJET 4100N	1
HP	LASERJET 420	1
HP	LASERJET 4250	28
HP	LASERJET P3005	61
HP	P100	1
intermec	EASYCODER C4	121
KODAK	8500 DIGITAL PHOTO PRINTER	1
KYOCERA	FS 9100DN	1
MITA		
LEXMARK	2381-002	1
LEXMARK	2481 PLUS	1
LEXMARK	3200	1
LEXMARK	E350D	1
LEXMARK	E352DN	2
LEXMARK	FORMS PRINTER 2481	1
LEXMARK	STYLUS COLOR 400	4
LEXMARK	Z24	1
LEXMARK	Z43	4
LEXMARK	Z515	1
MINOLTA	PAGEPRO 1100L	4

OLIVETTI	JP 470	1
OLIVETTI	JP450	1
SAMSUNG	ML-1210	10
SCONOSCIUTA	SCONOSCIUTO	1
TALLY	T2130	1
TALLY	T9112	1
TALLY	T9212	1
XEROX	PHASER 8200	1
XEROX	STYLUS COLOR 400	1
ZEBRA	DA402	3
ZEBRA	LP 2844-Z	3
ZEBRA	S600	1
ZEBRA	TLP 2844	1
ZEBRA	TPL 2844	1
	Totale	**1492**

Elenco Server aziendali

BULL	ESCALA POWERPC
BULL	ESCALA POWERPC
BULL	ISM SERVER 585 POWERPC
CLONE	
COMPAQ	PROLIANT 800
COMPAQ	PROLIANT ML350
COMPAQ	PROLIANT ML530
DELL	Power Edge 1800
FUJITSU Siemens	F250
FUJITSU Siemens	PRIMEPOWER 200
FUJITSU Siemens	PRIMERGY
FUJITSU Siemens	PRIMERGY
FUJITSU Siemens	PRIMERGY (?)
FUJITSU Siemens	PRIMERGY 250
FUJITSU Siemens	PRIMERGY E200
FUJITSU Siemens	PRIMERGY E200
FUJITSU Siemens	PRIMERGY E200
FUJITSU Siemens	PRIMERGY E200
FUJITSU Siemens	PRIMERGY F200
FUJITSU Siemens	PRIMERGY F250
FUJITSU Siemens	Primergy F250
FUJITSU Siemens	Primergy F250
FUJITSU Siemens	PRIMERGY H450
FUJITSU Siemens	PRIMERGY P250
FUJITSU Siemens	PRIMERGY P250
FUJITSU Siemens	PRIMERGY P250 GE
FUJITSU Siemens	Primergy RX200S2
FUJITSU Siemens	Primergy RX300S2
FUJITSU Siemens	Primergy RX300S2
FUJITSU Siemens	Primergy RX300S2
FUJITSU Siemens	Primergy RX300S2

FUJITSU Siemens	Primergy RX600S2
FUJITSU Siemens	Primergy RX600S2
FUJITSU Siemens	Primergy RX600S3
FUJITSU Siemens	Primergy RX600S3
FUJITSU Siemens	PRIMERGY TX200f
FUJITSU Siemens	PRIMERGY TX200f X
FUJITSU Siemens	PRIMERGY TX200R
FUJITSU Siemens	PRIMERGY TX200R
FUJITSU Siemens	PRIMERGY TX200R
FUJITSU Siemens	PRIMERGY TX200R3
FUJITSU Siemens	Primergy TX200S2r
FUJITSU Siemens	Primergy TX200S2r
FUJITSU Siemens	Primergy TX200S2r
FUJITSU Siemens	Primergy TX200S2r
FUJITSU Siemens	Primergy TX200S2r
FUJITSU Siemens	Primergy TX200S2r
FUJITSU Siemens	Primergy TX200S2r/X
FUJITSU Siemens	Primergy TX200S2r/X
FUJITSU Siemens	Primergy TX200S2r/X

FUJITSU Siemens	Primergy TX300S2
FUJITSU Siemens	Primergy TX300S2
FUJITSU Siemens	Primergy TX300S2
FUJITSU Siemens	Primergy TX300S2
FUJITSU Siemens	Primergy TX300S2
FUJITSU Siemens	RX200S3
FUJITSU Siemens	RX300S3
FUJITSU Siemens	RX300S3
FUJITSU Siemens	RX300S3
FUJITSU Siemens	RX600S3
FUJITSU Siemens	RX600S3
FUJITSU Siemens	RX600S3
FUJITSU Siemens	RX600S3
FUJITSU Siemens	RX600S3
FUJITSU Siemens	SCENIC
FUJITSU Siemens	TX200
FUJITSU Siemens	TX200
FUJITSU Siemens	TX200R
FUJITSU Siemens	TX200R
FUJITSU Siemens	TX300R2
HELWETT-PACKARD	NET SERVER LH PRO
HP Compaq	Proliant ML350T
IBM	system x3850
IBM	system x3850
IBM	X346
IBM	X346
IBM	X346
IBM	X346
IBM	X366
IBM	X366
INTERCOMP	SERVER 5000
INTERCOMP	
OLIDATA	AMD 64 Athlon
OLIDATA	AMD Sempron
OLIVETTI	SYSTEMA 160/N
SUN	SUNFIRE X2100
ZENITH	EXPRESS 5800 LS 2400
ZENITH	EXPRESS 5800 LS 2400
ZENITH	EXPRESS 5800 LS1200
ZENITH	EXPRESS 5800 LS2400
ZENITH	EXPRESS 5800 LS2400
ZENITH	EXPRESS 5800 LS2400
ZENITH	EXPRESS 5800 MC2400
ZENITH	EXPRESS 5800 MC2400R
ZENITH	SCENIC
ZENITH	Z-SERVER MX
ZENITH	Z-SERVER WL

Librerie di Backup

Quantità		
2	Adic	Scalar 24 SCSI
3	Tandberg	Autoloader SLR 100

Elenco degli applicativi aziendali

Applicativo	Unità Operative interessate
HsWeb (Cartella infermieristica)	Reparti e ambulatori ospedalieri Reparti
Med's Office (Agenda ambulatoriale)	e ambulatori ospedalieri Reparti e
Med's Office Web (Agenda ambulatoriale)	ambulatori ospedalieri Reparti
Infoclin (Cartella Medica)	ospedalieri e Comparti operatori
Screening	Consultori
Pronto Soccorso Web	Pronto Soccorso e Accettazione
ADT Web	Pronto Soccorso e Accettazione e Reparti
ADI	Assistenza Domiciliare Medicina di Base
WebCup	
Tickets PS	Sportelli aziendali
Medicina Di Base	Medicina di Base
Sister	Sert
Aster Med Leg	Invalidi Civili e Rinnovo patenti
Gestione Incassi	Uffici Cassa
Magicweb	Reparti ospedalieri
RA2000	UU.OO. Radiologia
Sienet SKY	UU.OO. Radiologia, Ortopedia
Medicina Di Base	Medicina di Base
Teseo	Economato
Medicina Nucleare	Medicina Nucleare
Wirtec	Assistenza Domiciliare
3p Studio-Efeso	Salute Mentale
Elea	Neuropsichiatria infantile
WinSap	Anatomia Patologica
Wincoder Drg Finder	Bobbio
Tesi	Centro Trasfusionale
Gepadial	Nefrologia e Dialisi
Doc Suite	Protocollo

SI2	Turni infermieristici
Job Time	Personale
Gestione Paghe	Personale
Quani SDO	Ufficio DRG
TraumaCenter	Dipartimento di Emergenza-Urgenza 118
arva4 e arva5	assistenti sanitari
mif99	assistenti sanitari O.C. Castel San Giovanni
winlab	Centro Trasfusionale
Simpi	Sociale-neuropsichiatria Infantile
Psy system3	Sociale-neuropsichiatria Infantile
winfood	Medicina ERI e dietiste
sentpay	U.O. Bilancio e altre postazioni
TaoWeb	Laboratorio Analisi
Egeo	U.O. Qualità e Formazione
EncoPro	U.O. Bilancio, U.O. Acquisizione Beni e Servizi, U.O. Servizi Generali e Logistici, Dipartimento Tecnico
Guardia Medica	Direzione Amministrativa Rete Territoriale
Argos	U.O. Prevenzione e Protezione SerT
Winsimet	
Anagrafe Assistiti	Direzione Amministrativa Rete Territoriale
Anagrafe Dipendanti	U.O. Sistemi Informativi e Tel. Comitato
PraticheWeb	Etico
DasiLab	Laboratori di Analisi
DISP	Dipartimento di Sanità Pubblica

Elenco dei dispositivi telefonici e delle linee telefoniche

Elenco Linee telefoniche

Comune	Sede	Tipologia e numero linee
Piacenza	Ospedale Civile Via Taverna, 49	Linee interne 717
Piacenza	Ospedale Civile Via Taverna, 49	Linee Urbane 27
Piacenza	Via Taverna, 48	Linee interne 26
Piacenza	Cantone del Cristo, 50	Linee interne 397
Piacenza	Cantone del Cristo, 50	Linee Urbane 1
Piacenza	Cantone del Cristo, 50	Linee VOIP 10
Piacenza	Cantone del Cristo-Malattie infettive	Linee interne 87 (di cui 15 DECT)
Piacenza	Sede di Via Leonardo da Vinci, 35	Linee interne VOIP 6
Piacenza	Sede di Corso Vittorio Emanuele, 169	Linee interne 169
Piacenza	Sede di Corso Vittorio Emanuele, 169	Linee Urbane 20
Piacenza	Sede di Via Anguissola, 5	Linee Urbane 4
Piacenza	Sede di P.le Milano, 2	Linee interne 218
Piacenza	Sede di Via Gadolini, 36	Linee interne 48
Piacenza	Sede di Via Gadolini, 36	Linee Urbane 6
Fiorenzuola d'Arda	Via Garibaldi/Via Roma – Ospedale	Linee interne 159
Fiorenzuola d'Arda	Via Garibaldi/Via Roma – Ospedale	Linee Urbane 18
Fiorenzuola d'Arda	Via Rossi, 17	Linee interne 22
Fiorenzuola d'Arda	Via Corridoni, 9	Linee interne 8
Fiorenzuola d'Arda	Via Scapuzzi, 4	Linee interne 19
Fiorenzuola d'Arda	Via Scapuzzi, 4	Linee Urbane 1
Fiorenzuola d'Arda	Via S. Rocco, 39	Linee interne 36
Fiorenzuola d'Arda	Via S. Rocco, 39	Linee Urbane 3
Fiorenzuola d'Arda	P.le Taverna, 2	Linee interne 20
Fiorenzuola d'Arda	P.le Taverna, 2	Linee Urbane 4
Fiorenzuola d'Arda	altre Sedi minori	Linee Urbane 7
Cortemaggiore	Ospedale	Linee interne 60
Cortemaggiore	Ospedale	Linee Urbane 4
Villanova	Ospedale	Linee interne 43
Cortemaggiore	Ospedale	Linee Urbane 1
Monticelli d'Ongina	Via Garimberti, 1	Linee interne 32
Monticelli d'Ongina	Via Garimberti, 1	Linee Urbane 11
Lugagnano Val d'Arda	Via Bersani 27	Linee interne 12
Lugagnano Val d'Arda	Via Bersani 27	Linee Urbane 10
Morfasso	Sede	Linee Urbane 2
Castel San Giovanni	Ospedale civile	Linee interne 199
Castel San Giovanni	Ospedale civile	Linee Urbane 18
Castel San Giovanni	Via G. Bruno, 2	Linee interne 48
Castel San Giovanni	Via G. Bruno, 2	Linee Urbane 5
Castel San Giovanni	Via I Maggio, 6	Linee interne 34
Castel San Giovanni	Via I Maggio, 6	Linee Urbane 4
Castel San Giovanni	Via Amendola, 2	Linee interne 1
Castel San Giovanni	Via Amendola, 2	Linee Urbane 3
Castel San Giovanni	Altre Sedi minori	Linee Urbane 7
Borgonovo val Tidone	Ospedale	Linee interne 68
Borgonovo val Tidone	Ospedale	Linee Urbane 7
Val Tidone	Altre Sedi minori	Linee Urbane 1
Bobbio	Ospedale	Linee interne 58
Bobbio	Ospedale	Linee Urbane 2
Alta Val Trebbia	Altre Sedi minori	Linee Urbane 5
Bassa Val Terbbia	Altre Sedi minori	Linee Urbane 3

Bettola	Via circonvallazione, 17	Linee interne 13
Bettola	Via circonvallazione, 17	Linee Urbane 1
alta Val Nure	Altre Sedi minori	Linee Urbane 15
bassa Val Nure	Altre Sedi minori	Linee Urbane 1
Rottofreno	S.Nicolò Via Curiel/XXV aprile, 49	Linee interne 11
Rottofreno	S.Nicolò Via Curiel/XXV aprile, 49	Linee Urbane 3
Podenzano		Linee interne 16
Podenzano		Linee Urbane 3
Carpaneto P.no	Via San Confalonieri	Linee Urbane 10

Elenco Telefoni Pubblici

Piacenza: n° 28
Fiorenzuola: n° 6
Cortemaggiore: n° 2
Bobbio: n° 1
Villanova: n° 1
Castel S. Giovanni: n° 3
Borgonovo: n° 2

Numero apparati di telefonia mobile: 350