**Scaletta per l’implementazione dei siti e delle strategie di recupero**

**Scopo strategie**: ripristinare le operazioni IT in modo veloce ed efficace dopo che è avvenuta un’interruzione.

In base all’impatto dell’interruzione e ai tempi massimi di interruzione riportati nella BIA, il CPC decide quali strategie implementare. L’uso di una strategia dipende anche dai costi, dati tempi di interruzione consentiti, dalla sicurezza.

In base all’impatto identificato nella BIA per il servizio down, si decide una strategia e la si integra nell’architettura durante le fasi di progettazione e implementazione del SLC. Il tipo di approccio scelto dipende dal problema, dal tipo di sistema e dai sui requisiti operativi. Si fa notare che i metodi di ripristino dovrebbero considerare e potrebbero includere accordi commerciali con vendor di siti cold, warm e hot, mobile o mirrored, accordi reciproci tra imprese simili (DR), SLA con i venditori di apparecchiature. Inoltre devono essere considerate tecnologie come RAID, automatic falir-over, e UPS quando si sviluppa una strategia di ripristino.

**Cose da tenere conto**

**Importanza dei backup**

I dati devono essere backuppati regolarmente. Ci devono essere polizze che specificano la frequenza dei backup basandosi sulla criticità dei dati contenuti nelle specifiche macchine (per ogni server indicare una frequenza di backup e la tipologia, in base alla sua criticità). Una polizza di backup deve includere:

* Dove i dati vanno memorizzati (in quale luogo);
* Convenzione di nome di file;
* Frequenza di rotazione dei media;
* Metodi per trasportare i dati fuori dal sito;
* In che supporto memorizzare i dati (disco, nastro, disco ottico).

La polizza di backup decisa dipende dal sistema e dai dati che esso memorizza, inoltre dipende dai requisiti di integrità.

È buona pratica immagazzinare i backup su un sito esterno. Se si utilizza un sito esterno, i dati vengono backuppati all’interno dell’organizzazione, etichettati, impacchettati e trasportati al sito esterno. Quando i dati serviranno, l’organizzazione contatterà il sito esterno per il trasporto dei dati. Infatti i magazzini di dati commerciali spesso offrono il trasporto di dati e servizi di ripristino.

**Scelta di un sito esterno**

* Area geografica: valutare la distanza per capire se lo stesso disastro potrebbe colpire anche il sito esterno;
* Accessibilità: tempo necessario per riottenere i dati;
* Sicurezza: confidenza degli impiegati del centro dati;
* Ambiente: condizioni del centro dati;
* Costi: costi di spedizione, tasse operative, tipi di servizi di recovery offerti in caso di disastro.

**Siti alternativi**

Sono da considerare per quei tipi di disastri con effetti a lungo termine che, anche se rari, sono sempre possibili. Quindi il piano deve includere strategie per ripristinare e eseguire le operazioni del sistema su un sito alternativo per un periodo di tempo esteso. Esistono tre tipi di siti alternativi, siti dedicati e utilizzati dall’organizzazione, accordi reciproci con un’organizzazione esterna o interna, contratti con fornitori di questo tipo di servizi. Questi tre tipi possono essere categorizzati in base alla loro prontezza operativa. Basandosi su questo i siti possono essere cold, warm, hot, mobile o mirrored.

* Cold: sito con spazio e infrastruttura (energia, telecomunicazioni) adeguata per supportare il sistema IT. Il sito non contiene apparecchiatura IT e d’ufficio (telefoni,stampanti). L’organizzazione che intende usare un cold site deve occuparsi di installare l’apparecchiatura necessaria e le telecomunicazioni;
* Warm: sono parzialmente forniti e contengono qualcuno o tutti gli hw,sw,telecomunicazioni e sorgenti di energia. È mantenuto in uno stato operativo pronto a ricevere lo spostamento del sito. Potrebbe essere necessario preparare il sito ad ospitare personale di recupero e sistema IT. In alcuni casi un sito warm può fornire servizi quotidiani normali e in caso di disastro queste funzioni vengono rimpiazzate per supportare il recupero del sistema;
* Hot: spazi propriamente dimensionati per supportare i requisiti di sistema e configurati con l’hw,sw,infrastruttura e personale necessari. Sono disponibili 24 h su 7 giorni la settimana. Il personale al suo interno prepara il tutto per l’arrivo del sistema non appena viene notificato dell’attivazione del piano;
* Mobile: consistono in siti trasportabili e con grandezza customizzata per contenere specifiche telecomunicazioni e apparecchiatura IT necessari a soddisfare i requisiti del sistema. Di solito il sito è contenuto in un furgone che può essere trasportato alla locazione alternativa desiderata. Per essere una valida soluzione di recupero, necessita di essere progettato in anticipo con il vendor e di essere regolamentato con uno SLA. Serve perché il tempo necessario per configurare il sito può essere lungo e il tempo per poi raggiungere la locazione potrebbe eccedere quello massimo di interruzione;
* Mirrored: sono completamente ridondati con informazione totale e disponibile in tempo reale. Sono identici al sito primario in tutti gli aspetti tecnici. Forniscono il massimo livello di disponibilità perché i dati sono sempre consistenti tra i due sistemi. Sono tipicamente progettati, costruiti e mantenuti dall’organizzazione stessa.

**Considerazioni sui siti**

Sono differenti per costi e tempi di disponibilità. Il mirrored è il più costoso ma è sempre dispinibile. Cold è il meno costoso ma richiede tempo aggiuntivo per installare l’apparecchiatura necessaria. Un buon compromesso potrebbero essere i warm che sono parzialmente forniti di apparecchiatura IT. Da notare che in alcuni casi i siti mobili possono essere spostati alla locazione desiderata in 24 ore. Però il tempo di installazione può aumentare il tempo di risposta. D’altra parte i siti fissi richiedono tempo per il trasporto del personale all’interno del sito. Inoltre un sito fisso dovrebbe essere in un’area geografica che non possa essere colpita dallo stesso disastro che colpisce il sito primario. La tabella a pagina 22 della guida BOMBA aiuta a capire quale tipo di sito alternativo utilizzare per soddisfare i requisiti dell’organizzazione, sempre basandosi sulla BIA e sul denaro disponibile. I siti devono essere valutati in modo che la sicurezza, gestione, operatività e controlli tecnici possano essere compatibili con il sito primario.

**Altra categoria**

Inoltre, i siti alternativi possono essere posseduti e gestiti dall’organizzazione stessa oppure essere siti commerciali disponibili sotto contratto. Se si firma un contratto con un vendor commerciale devono essere negoziati i tempi di testing, i requisiti di sicurezza, i requisiti hardware, di telecomunicazioni, i servizi supportati e i giorni di ripristino (quanto tempo l’organizzazione può occupare il sito durante il periodo di ripristino). È da tenere conto che il sito potrebbe essere affittato a più organizzazioni e che in caso di disastro non tutte possono starci contemporaneamente. Bisogna negoziare anche il verificarsi di tali situazioni.

**Contratti reciproci**

Due o più organizzazioni con simili o identiche configurazioni IT e tecnologie di backup possono firmare un contratto formale per fare da fornitori di siti alternativi l’un l’altro o firmare un contratto insieme per un sito esterno. Questo tipo di sito si ottiene con accordo reciproco o MOU. Un accordo reciproco deve essere fatto con attenzione perché bisogna avere la sicurezza che ogni sito sia in grado di supportare l’altro anche in caso di disastro (quindi comporterebbe lavoro doppio). I test dovrebbero essere condotti nel sito del partner per valutare se il sito del partner potrebbe riuscire a tenere il carico di lavoro più alto, per verificare la compatibilità tra i sistemi e le configurazioni di backup, se le telecomunicazioni sono sufficienti, se le misure di sicurezza sono compatibili.

Un MPU dovrebbe essere sviluppato in base ai bisogni dell’organizzazione e alle capacità del sito partner. Il legale di entrambe le parti deve firmare l’accordo. Gli elementi per stilare un accordo sono presenti a pagina 22.

**Possibilità di trasporto verso un sito alternativo**

Nel caso in cui il sistema IT sia danneggiato o distrutto oppure il sito primario non disponibile, l’hw e il sw necessari devono essere attivati e procurati velocemente e consegnati alla locazione alternativa. Esistono tre strategie per il trasporto dell’apparecchiatura. Nel selezionare una delle strategie bisogna tenere conto che la disponibilità di trasporto può essere limitata o temporaneamente bloccata a causa del disastro.

* Accordi con vendor: nello svliluppare un piano di Contingency, gli SLA per hw, sw e i vendor di supporto dovrebbero essere fatti per mantenere il servizio durante l’emergenza. Lo SLA specifica la velocità con la quale il vendor deve rispondere dopo essere stato notificato, la priorità con cui è necessario spedire l’apparecchiatura sormontando le vendite normali quotidiane. In pratica è un contratto ad esempio con media world che in caso di disastro si deve impegnare a bloccare le vendite per supportare l’azienda in difficoltà. Bisogna negoziare anche la priorità dell’organizzazione rispetto le altre che si sono affidate allo stesso vendor.;
* Inventario: si compra l’apparecchiatura necessaria in anticipo con ottica pro attiva, ossia prevenire è meglio che curare. Questa viene messa in una posizione fuori dall’organizzazione, ad esempio in un sito alternativo dove le operazioni di recupero avranno luogo (warm, mobile), oppure in un luogo dove poi dovranno essere però spedite al sito alternativo. Lo svantaggio è che si spendono i soldi subito e che l’apparecchiatura può diventare obsoleta perché la tecnologia cambia in fretta. Questi sono sempre stati gli aspetti negativi di un’ottica pro attiva;
* Apparecchiatura compatibile esistente: apparecchiatura già esistente e utilizzata in un hot site. Accordi presi con gli hot site specificano che l’apparecchiatura compatibile sarà disponibile per usi di emergenza dell’organizzazione. Da qua si capisce che un hot site potrebbe essere già pronto e affittato interamente con già tutto dentro, non si parla solo di affittare un capannone, ma un’intera azienda informatica.

**Considerazioni**

Valutando tra le possibili scelte bisogna tenere conto che comprare quando è necessario è buono per i costi ma richiede molto tempo per il trasporto e il setup. D’altra parte avere già le apparecchiature è costoso ma si risparmia tempo nel setup. Anche qui bisogna considerare in base agli impatti e ai tempi di interruzioni scoperti tramite la BIA e bisogna considerare la possibilità di un disastro ambientale. Una lista dettagliata dell’apparecchiatura necessaria dovrebbe essere mantenuta nel piano.

**Ruoli e responsabilità**

Dopo aver selezionato e implementato la strategia di ripristino del sistema, il coordinatore deve predisporre i team appropriati per implementare la strategia. Ogni team deve essere allenato e pronto all’evento di un’interruzione che richiede l’attivazione del piano. Il personale di recupero dovrebbe essere assegnato a uno degli specifici team che risponderanno all’evento, alle capacità di recupero e che porteranno il sistema alle operazioni normali. Per far questo, è importante che i team capiscano l’obiettivo specifico del team all’interno del processo di recupero, ogni step che deve eseguire e come deve interagire con gli altri team. I tipi di team necessari dipendono dal sistema. La dimensione dei team dipende dall’organizzazione. È possibile che una strategia richieda più team.

N.B. Il personale viene scelto in base alle proprie abilità e conoscenze in materia. Il team viene scelto in base a ciò che le persone svolgono durante le operazioni normali. I team devono avere una dimensione sufficiente da permettere la loro disponibilità anche in caso di assenza di personale. Inoltre il personale di ogni team deve avere familiarità con le funzioni dei team con i quali si coordina. Bisogna tenere conto che un disastro potrebbe compromettere l’utilizzo di tutto il personale interno e quindi per attivare il piano è necessario per forza di cose del personale esterno. Ogni team ha un leader che supervisiona le operazioni e agisce da rappresentante del team. Approva le decisioni del team. Devono essere disponibili dei leader alternativi nel caso in cui i primari non fossero disponibili (mettere nei contatti anche questi->ma anche no->possiamo dire che nel caso in cui uno si ammalasse viene sostituito).

Il management Team è necessario per fare da guida in caso di disastro o emergenza. È responsabile di attivare il piano (se ne occupa il senior) e supervisionare l’esecuzione delle operazioni d’emergenza. Supervisiona le fasi di test ed esercizio del piano e facilita la comunicazione tra i vari team.

Importante anche la linea di successione che serve a capire chi si deve assumere le responsabilità se l’autorità principale non è disponibile. Non ci devono essere conflitti di responsabilità e bisogna scendere fino alla fine della catena.

**Considerazioni sul costo**

Il CPC dovrebbe assicurare che la strategia scelta sia implementata efficacemente con il personale disponibile e le risorse finanziarie. Quindi bisogna fare attenzione al denaro che l’organizzazione ha a disposizione per implementare le strategie e costruire gli stabilimenti d’emergenza. Devono essere presi in considerazioni i costi di siti alternativi, rimpiazzo apparecchiature e le opzioni di immagazzinamento, tenendo conto delle limitazioni di budget dell’organizzazione. Inoltre bisogna tenere in considerazione il costo della pianificazione, contratti con siti alternativi, costo del supporto dei contrattor. Il budget deve tenere conto e deve essere sufficiente per hw, sw, viaggio e spedizione, test, programmi di allenamento, servizi contrattati. Devono essere valutate delle analisi di costo beneficio per trovare la strategia di ripristino ottima. Guardare la tabella di costi a pag. 27.

**Fase di ripristino**

Le procedure di ripristino iniziano una volta che il piano è stato attivato, la valutazione sul danno è stata completata, il personale notificato e i team mobilizzati. L’obiettivo delle strategie è applicare misure d’emergenza per eseguire capacità IT temporanee, riparare danni al sistema originale e ripristinare le capacità del sistema originale. Una volta completata questa fase il sistema IT sarà operativo e verranno supportate le funzioni descritte nel piano. A seconda della strategia le funzioni potrebbero includere ripristino e operatività in sistemi alternativi, trasferimento in siti alternativi.

Sequenza delle attività di ripristino

Bisogna capire la sequenza delle operazioni in base alle priorità identificate nella BIA. Prima si eseguono le strategie per le parti del sistema più a rischio e più importanti e poi si scende. Bisogna tener conto quindi anche dei tempi d’interruzione massima per evitare interruzioni che danneggino funzioni di business del sistema. Le procedure vengono descritte a step per permettere il ripristino delle componenti in ordine logico. Esempio, se la LAN cade, prima devono essere ripristinati i server principali e poi le stampanti per ultime. Per un application server, prima si ripristina il sistema operativo e poi le applicazioni e i loro dati (dati presi da un backup che potrebbe essere in un altro luogo). Le procedure includono anche coordinamento con altri team al verificarsi di certe situazioni:

* Azione non completata in tempo;
* Step chiave completato;
* Un oggetto deve essere procurato.

Se la condizione verificata richiede il trasferimento verso un sito alternativo alcuni materiali devono essere traferiti e procurati. Spedizione di backup media da uno storage esterno, hw, sw. Le procedure devono anche designare team appropriati e membri del team per coordinare la spedizione di apparecchiature, dati e record vitali. Inserire i recapiti dei vendor a fine sezione, mettere tutto in appendice per fare i fighi. Le procedure devono descrivere i requisiti di impacchettamento, trasporto e compravendita di materiali richiesti per ripristinare il sistema. Quindi come devono essere impacchettati e spediti i backup per esempio.

Come scrivere le procedure di ripristino

Devono essere scritte nel modo più dettagliato possibile. Considerazioni di ripristino sono trattate in seguito. Devono essere assegnate ad uno specifico team e seguire le seguenti azioni:

* Ottenere autorizzazioni per accedere ai depositi danneggiati;
* Notificare partner interni ed esterni associati al sistema;
* Ottenere il necessario provvigionamento d’ufficio e lo spazio di lavoro;
* Ottenere e installare i necessari componenti hardware;
* Ottenere e caricare i backup;
* Ripristinare i sistemi operativi e i software applicativi;
* Ripristinare i dati di sistema;
* Testare le funzionalità del sistema includendo controlli di sicurezza;
* Connettere il sistema alla rete;
* Rendere operativa l’apparecchiatura alternativa.

Le procedure devono essere scritte a step, nessuno step deve essere preso per assunto o omesso.

Scaletta

* Leggere la BIA e capire quali sono i componenti hw e sw critici. I sistemi con priorità alta sono quelli che devono essere ripristinati in tempo minore perché hanno tempi di interruzione minori e alti impatti per l’istituto;
* Stabilimento: Capiti i sistemi si procede con il capire quali backup devono essere fatti, dove memorizzare i dati, valutare anche se metterli in uno storage offsite e quindi se firmare un contratto con aziende apposite. Capire in seguito quali apparecchiature devono essere ridondate, quali server, quali router, quali sw, capire se c’è il tempo per trasferirli o se devono essere già disponibili sul sito alternativo. Se devono essere trasferiti, valutare un contratto con un’azienda che offre questo tipo di servizi. Se non devono essere trasferiti ma devono essere già nel sito, valutare un contratto con l’azienda che affitta il sito e l’apparecchiatura, ovviamente se il sito è esterno, come nel caso di hot stand by;
* Procedure: Capito cose mettere nei vari siti si procede con le procedure di ripristino. Si identificano i team necessari per il ripristino delle varie componenti nei vari siti e si fanno delle procedure a step che includano tutte le cose già scritte precedentemente.

**Considerazioni per stabilimento e procedure – capitolo 5**

Questa parte assiste il lettore nel selezionare, sviluppare e implementare specifiche strategie d’emergenza. Vengono discussi requisiti tecnici o fattori che il CPC dovrebbe considerare mentre pianifica una strategia. Poi vengono fornite delle soluzioni tecnologiche per ogni tipologia di piattaforma. In tutte le piattaforme vengono discusse:

* Frequenza dei backup e storage offsite per dati, applicazioni e sistemi operativi;
* Ridondanza di componenti di sistema critiche e capacità;
* Documentazione di configurazioni di sistema e requisiti;
* Interoperabilità tra componenti del sistema e tra sito primario e alternativo per velocizzare il ripristino del sistema;
* Configurare propriamente UPS e controlli ambientali.

**Considerazioni su postazioni e portatili**

I PC sono i normali PC che utilizziamo ogni giorno e nel caso dell’ospedale sono le postazioni di lavoro, ovvero quei PC progettati per essere utilizzati da una persona per volta. Sono la piattaforma più comune per i processi di routine e quindi sono elementi importati in un piano d’emergenza. Bisogna tenere in considerazione che possono essere fisicamente collegati alla LAN, possono accedere alla rete aziendale tramite accesso remoto.

Considerazioni d’emergenza

Le considerazioni dovrebbero enfatizzare la disponibilità, riservatezza e integrità dei dati. Per seguire questi requisiti bisogna considerare:

* Immagazzinare i backup su un sito esterno: i dati di backup dovrebbero essere immagazzinati esternamente al sito in un deposito sicuro e controllato. Se gli utenti salvano i dati su un sistema isolato e non connesso alla rete, bisogna tenere in considerazione che devono essere trasportati sul sito esterno. Una copia del piano, delle licenze sw, degli SLA con i vendor e contratti dovrebbero essere memorizzati con i dati di backup. La BIA dovrebbe aiutare a capire ogni quanto fare backup;
* Incentivare gli utenti a fare backup: se il backup non è automatizzato dalla rete, gli utenti devono essere incoraggiati a fare backup regolarmente;
* Fornire guide su come fare backup sui PC: istruire gli utenti a fare backup su cartelle specifiche facilita il tutto. In caso di ricostruzione della macchina, il tecnico saprà dove trovare i dati;
* Standardizzare hw e sw: il ripristino è più veloce se hw e sw sono standardizzati dall’organizzazione. Se non sono possibili standardizzazioni tramite l’organizzazione, è necessario standardizzare tramite il dipartimento o per tipo di macchina;
* Documentare le configurazioni di sistema e le info sui vendor: documentare le configurazioni di sistema aiuta nel ripristino del sistema. I contatti dei vendor aiutano in situazioni d’emergenza per comprare velocemente l’apparecchiatura di rimpiazzo;
* Coordinare con polizze di sicurezza e controlli di sicurezza: scegliendo la soluzione di contingenza più appropriata, controlli di sicurezza associati dovrebbero essere implementati nella soluzione per assicurare che durante un’interruzione di sistema, eseguendo la procedura di sicurezza non vengano compromessi dati sensibili;
* Usare i risultati della BIA: vengono utilizzati per scoprire i requisiti di ripristino della strategia.

Soluzioni di contingenza

Prima di tutto i dati della BIA per le applicazioni più importanti e i sistemi di supporto dovrebbero essere usati per determinare i requisiti di ripristino e le priorità da implementare. Le soluzioni di contingenza sono:

* Backup: è il mezzo più comune per assicurare la disponibilità di dati sui pc. Alcuni fattori dovrebbero essere presi in considerazione selezionando una soluzione di backup:
  + Interoperabilità apparecchiatura: il dispositivo di backup deve essere compatibile con il sistema operativo della piattaforma e dovrebbe essere facile da installare in differenti modelli e tipologie di PC;
  + Volume del storage: la quantità di dati da salvare dovrebbe determinare la soluzione di backup più opportuna;
  + Vita del media: valutare l’utilizzo e la durata di conservazione dei supporti. Superata la durata di conservazione non è possibile far affidamento a tali supporti per il backup;
  + Software di backup: il sw o il metodo di fare backup deve essere considerato. In certi casi l’applicazione di backup potrebbe essere una semplice copia manuale di dati tramite un file manager. In casi con grandi quantità di dati si può usare un’applicazione di terze parti per automatizzare e calendarizzare i backup;

Bisogna capire anche quale metodo utilizzare per fare i backup:

* Floppy disk: è la soluzione più economica ma i driver hanno poca capacità di immagazzinamento e sono lenti;
* Nastri: non sono comuni nel backup dei PC ma sono una soluzione per grandi quantità di dati. Sono automatizzati e richiedono applicazioni di terze parti per fare il backup. Sono relativamente a basso costo;
* Cartucce rimovibili: non comuni per i PC, sono veloci e la loro portabilità permette flessibilità;
* CD: i CD read-only sono lo standard per i PC. Però bisogna tenere conto che non tutti i PC supportano i CD nativamente. Non costano molto e hanno capacità più alte dei floppy disk. Per leggere un CD è sufficiente il sistema operativo mentre per scriverlo è necessario anche del sw;
* Network storage (cloud): se il PC è connesso alla rete è possibile valutare questa alternativa:
  + Disco in rete: è un server con capacità di immagazzinamento. La quantità di immagazzinamento dipende dalla quantità di spazio del server o dalla quantità assegnata all’utente. Se gli utenti memorizzano i file su un disco in rete allora anche questo disco deve essere backuppato tramite la rete o un programma di backup per server;
  + Device per lo storage in rete: un sistema di backup in rete può essere configurato per backuppare i drive locali su un PC in rete.
* Replica o sincronizzazione: è un metodo di backup per i pc portatili. I pc dovrebbero essere collegati ad un altro pc per replicare i dati desiderati da un pc all’altro;
* Internet backup: è il cloud. Permette agli utenti di fare backup su una locazione remota pagando una tassa. Una app è installata sul pc e permette all’utente di schedulare i backup, selezionare i file e le cartelle per il backup, e stabilire uno schema di archiviazione per prevenire la sovrascrittura di file. Il vantaggio è che l’utente non deve acquistare hardware o media per fare il backup.

Oltre ai dati, le organizzazioni dovrebbero salvare anche i driver di sistema, infatti i sw e le licenze per il sw vengono memorizzati su una locazione secondaria. Le applicazioni custom-built dovrebbero essere salvate e immagazzinate su una locazione alternativa o backupate con uno dei metodi di sopra. Le istruzioni per recuperare questo tipo di applicazioni su un sito alternativo dovrebbero essere ben documentate.

Bisogna inoltre considerare l’utilizzo di chiavi di cifratura nelle strategie di backup. Se queste chiavi vengono memorizzate nel PC, i dati possono diventare non recuperabili se il PC viene corrotto.

Poiché i portatili possono essere rubati, la cifratura deve essere utilizzata per proteggere i dati su un pc rubato. È possibile fornire un secondo disco per quando si esce con il pc, con le minime applicazioni utili a lavorare, in modo che in caso venga rubato, la perdita di dati sensibili è minima.

* Imaging: è un’altra soluzione di contingenza. Una immagine standard per PC può essere memorizzata e può essere ricaricata su un PC corrotto. L’immagine installerà le applicazioni e le impostazioni nell’immagine, tuttavia tutti i dati nel PC verranno persi. Per questo motivo gli utenti devono essere incoraggiati ad effettuare backup. Poiché le immagini possono essere molto grandi, uno spazio dedicato sullo storage di un server può essere allocato per le sole immagini. Per diminuire il numero di immagini necessarie nel caso in cui più pc vengano corrotti si possono standardizzare i modelli di PC e le loro configurazioni. Se un trasferimento è necessario, le configurazioni e le applicazioni base dei PC dovrebbero essere ben documentate nel piano di contingenza.

Il sistema e i suoi dati possono essere corrotti da un fallimento nell’energia elettrica. Un PC può essere configurato con due fornimenti di energia per prevenire la corruzione. I due power supply dovrebbero essere utilizzati contemporaneamente in modo che se uno fallisce l’altro è già pronto.

UPS proteggono il sistema se viene persa l’energia elettrica. Forniscono fino a 60 minuti di tempo per permettere uno spegnimento in sicurezza del sistema. Sono una buona soluzione di contingency per i server ma non per i PC a cause del loro costo.

**Considerazioni di contingenza per i server**

Supportano la condivisione di file e l’immagazzinamento, il processamento dei dati, hosting di applicazioni, stampanti, controllo d’accesso, autenticazione e connettività per accesso remoto. Gli utenti accedono al server mediante i PC connessi per accedere alle risorse che esso mette a disposizione.

Considerazioni di contingenza

Siccome i server possono hostare molte applicazioni critiche, la perdita di un server può causare una grande perdita per i processi di business. Devono essere considerate le seguenti pratiche:

* Salvare i backup e il sw in un sito esterno: i media di backup e il sw dovrebbero essere memorizzati su un sito esterno, sicuro e controllato;
* Standardizzare hw e sw: il ripristino del sistema può essere reso più veloce se hw e sw sono standardizzati tramite l’organizzazione. Le configurazioni standard dovrebbero essere documentate nel piano. Uno standard permette di mettere mano sul server per il ripristino nella stessa maniera per tutti i server;
* Documentare le configurazioni di sistema e i vendor: se si documentano le configurazioni di sistema risulterà più facile ripristinare lo stesso. I venditori di hw essenziale, sw e altri componenti devono essere identificati nel piano;
* Coordinare con polizze di sicurezza e controlli di sicurezza: controlli per verificare che l’esecuzione della soluzione di contingenza non comprometta dati sensibili;
* Usare i risultati dalla BIA: i requisiti di ripristino sono determinati dagli impatti e le priorità identificati nella BIA.

Soluzioni di contingenza per i server

La pianificazione d’emergenza dei server dovrebbe enfatizzare la disponibilità dei servizi di rete forniti dal server. Nel selezionare la soluzione anche la riservatezza dei dati dovrebbe essere considerata. Per prevenzione funzioni critiche non dovrebbero essere messe in server con funzioni non critiche se è possibile. Per esempio, un server dedicato ad una certa applicazione, dovrebbe fornire solo tale applicazione e non anche altre risorse.

Come per i PC, anche i server possono essere backupati regolarmente. Possono essere backuppati in un sistema distribuito dove ogni server ha il suo drive dedicato o in sistema centralizzato dove un device per backup centralizzato è installato su un server. Esistono tre tipologie di backup per i server:

* Full: cattura tutti i file sul disco o sulla cartella scelta per il backup. Il tempo richiesto per questa tipologia di backup può essere molto lungo. Un backup di questa tipologia su file che non vengono cambiati frequentemente può portare ad un’eccessiva e non necessaria memorizzazione di dati;
* Incremental: cattura file che sono stati creati o modificati dopo l’ultimo backup. Permette un uso più efficiente dello storage e ha una velocità maggiore di backup;
* Differential: cattura file creati o modificati dopo l’ultimo full backup. Richiede meno tempo per essere completato rispetto ad un full backup, richiede meno media per il recupero dei dati rispetto al backup incrementale. Però richiedono più tempo per essere completati rispetto ai backup incrementali.

Può essere utilizzata una combinazione di backup in base alle configurazioni di sistema e ai requisiti di ripristino. Per sviluppare il calendario di backup del server, le seguenti domande devono essere considerate:

* Dove i dati vengono salvati?
* Quali dati?
* Quanto di frequente?
* Quanto velocemente i dati vengono recuperati in caso di emergenza?
* Chi è autorizzato a prelevare i dati?
* Quanto tempo ci vuole per ottenerli?
* Dove deve essere consegnato il media?
* Quali controlli servono per preservare il media?
* Qual è il media più appropriato per il backup?
* Quali tipi di media readers ci sono nel sito alternativo?

I media di backup dovrebbero essere immagazzinati in un sito esterno sicuro e controllato. Quando si seleziona tale sito, le ore di locazione, facilità di accesso al media, limitazioni fisiche di immagazzinamento e i termini di contratto dovrebbero essere presi in considerazione. È importante che il media venga prelevato su base regolare dal sito esterno e testato per assicurare che i backup vengono fatti correttamente. Leggendo la BIA si capisce ogni quanto tempo i media devono essere testati. Tutti i media devono essere etichettati univocamente in modo da assicurare che i dati richiesti siano recuperati velocemente in caso di emergenza. Una buona strategia per etichettare i media è quella di mettere il giorno mese e anno di creazione del backup.

Sebbene inserire i media di backup su un deposito esterno permetta il ripristino del sistema, i dati aggiunti o modificati sul server dopo l’ultimo backup potrebbero andare persi durante un’interruzione o un disastro. Per evitare questa potenziale perdita, la strategia di backup deve essere complementata con soluzioni di ridondanza.

RAID

Fornisce la ridondanza dei dischi e diminuisce il tempo medio tra i fallimenti. Sono usati per mascherare i fallimenti del disco. RAID aumenta la performance e l’affidabilità mettendo i dati su più dischi invece che uno solo. RAID può essere implementato via hw o sw e in ogni caso viene visto come un unico disco dal sistema operativo. Lo swap dei dischi può essere fatto senza spegnere il sistema. Vengono utilizzate tre tecnologie di ridondanza:

* Mirroring: con questa tecnica il sistema scrive i dati contemporaneamente in dischi separati. In pratica ogni dato scritto viene ridondato su più dischi. Il downtime è minimo ed è semplice ripristinare i dati. Se un disco fallisce, il sistema può operare da un disco funzionante o può utilizzare un disco per la richiesta di lettura e uno per altre richieste. Ha un’elevata tolleranza ai guasti e può essere implementato tramite un controller hw RAID o tramite il sistema operativo;
* Parity: tecnica per determinare se i dati sono stati persi o sovrascritti. Ha una minore tolleranza ai guasti rispetto a mirroring. I dati possono essere protetti senza possedere una loro copia, che invece è richiesto da mirroring;
* Striping: migliora le performance del controller dell’array distribuendo i dati su tutti i dischi. Un elemento di dato è spezzato in più pezzi e ogni pezzo è distribuito su un disco diverso. La velocità di trasferimento è aumentata perché i dischi possono accedere ogni pezzo di dato simultaneamente. Il dato può essere spezzato in bytes oppure in blocchi di dimensione fissa.

Esistono sei livelli di RAID, ognuno con differenti configurazioni. I più comuni per la ridondanza dei dati sono RAID-1 e RAID-6:

* RAID-1: usa il mirroring per creare e immagazzinare copie identiche su due dischi. È semplice ed economico da implementare. Però il 50% di spazio di disco è perso per duplicare i dati;
* RAID-5: utilizza striping a livello di blocco e parità distribuita. La parità è scritta su tutti i dischi insieme al dato. Separare le informazioni sulla parità dal blocco attuale fornisce tolleranza ai guasti. Se un disco fallisce, i dati del disco fallito possono essere ricostruiti con i dati presenti sugli altri dischi.

RAID è una strategia efficace per ridondare i dischi. Tuttavia, la ridondanza di altre parti critiche del server, come il fornimento di energia, dovrebbe essere fornita. Il server dovrebbe essere equipaggiato di due power supplier, in modo che la seconda continui a supportare il server se quella principale si sovraccarica o diventa inutilizzabile.

Una seconda fonte di energia può proteggere contro un fallimento hardware ma non è efficace contro un fallimento di energia. Per assicurare energia a breve termine e proteggere contro fallimenti di enrgia, dovrebbe essere installato un UPS. Di solito fornisce abbastanza energia da permettere al sistema di spegnersi in sicurezza. Se è richiesta alta disponibilità, un generatore di energia a gas o diesel dovrebbero essere installati. Il generatore va installato nel sistema di energia elettrica e va configurato per partire automaticamente in caso di interruzione di energia elettrica.

Electronic vaulting e remote journaling

Sono tecnologie simili che forniscono capacità di backup aggiuntive facendo backup tu nastri remoti tramite link di comunicazione. Permettono minori tempi di ripristino e diminuiscono la quantità di dati persi se il server venisse danneggiato tra due backup. Con il vaulting elettrico il sistema è collegato ad un provider che permette di creare i backup offsite automaticamente. Può utilizzare dischi ottici, magnetici, tape library automatizzate. Con questa tecnologia i dati vengono trasmetti al vault elettronico se avvengono dei cambiamenti nei server tra i backup regolari.

Con il journaling remoto, i file di log vengono trasmetti ad una locazione remota. Nel momento in cui un server deve essere ripristinato, i file di log possono essere utilizzati per ripristinare cambiamenti su transazioni, applicazioni o database che sono successe dopo l’ultimo backup del server. Queste due tecniche richiedono un deposito esterno dedicato per ricevere le trasmissioni. Può essere l’hot site del sistema. Possono essere condotti su una connessione con larghezza di banda limitata a seconda della grandezza e della frequenza dei backup.

Server load balancing

Aumenta la disponibilità di server e applicazioni. Il traffico viene distribuito dinamicamente su un gruppo di server sui cui sta girando un’applicazione comune, in modo da non sovraccaricare un unico server. I sistemi di load balacing monitorano i vari server per capire a quale server inviare il traffico per aumentare le performance e la disponibilità in modo che nessun server sia sovraccarico. Può essere implementato con più server su un unico sito o più server su più siti diversi. Se i server sono su siti diversi, l’applicazione continuerà a girare anche se uno dei siti fallisce.

Replicazione di disco

I tempi di ripristino sono diminuiti perché i dati sono scritti in due dischi differenti per assicurare che due copie dei dati sono sempre disponibili. I dischi sono chiamati server protetto e server replicato. Esistono due diverse tecniche per il replicaggio di dati che hanno un RTO e un RPO differente. RTO è il massimo tempo accettabile prima che una non disponibilità del sistema abbia effetti negativi sull’organizzazione. RPO è il tempo nel quale il dato deve essere ripristinato per ricominciare il processing:

* Sincrono o mirroring: copia da disco a disco e mantenimento di file system e database applicando cambiamenti ogni volta che dei cambiamenti vengono fatti sul server protetto. L’RTO può essere di alcuni minuti fino ad alcune ore. Va usato per applicazioni critiche che non tollerano perdita di dati. Va usato nei casi in cui la larghezza di banda non infierisce sul trasferimento;
* Asincrono o shadowing: mantiene una replica del db e del fs continuamente catturando i cambiamenti da un log e portando questi cambiamenti sul server replicato. RTO può andare da alcune ore fino a un giorno. Deve essere usato per larghezze di banda inferiori e lunghe distanze dove la latenza di rete può accadere.

Per decidere la tecnica appropriata devono essere valutati la compatibilità, integrazione con altri prodotti complementari, costi, velocità di rilascio, impatti di performance.

**Considerazioni di contingenza per le reti locali**

Una LAN è posseduta da una singola organizzazione. Può essere piccola come un collegamento tra due pc o può supportare centinaia di utenti e molteplici server. La topologia usata dall’istituto è a stella, dove tutti i nodi sono connessi a un hub centrale. L’architettura invece è client server.

Considerazioni

Quando si sviluppa una strategia di ripristino per una rete locale bisogna prima seguire le informazioni per i computer e per i server e poi le seguenti informazioni:

* Documentazione sulla LAN: i diagrammi fisici e logici della LAN devono essere aggiornati. Il diagramma fisico dovrebbe visualizzare il layout fisico dello stabilimento che ospita la rete, il numero di cable jack dovrebbe inoltre essere documentato. Il diagramma logico dovrebbe presentare la LAN e i suoi nodi (questo c’è). Entrambi i diagrammi aiutano il personale di ripristino a recuperare la LAN velocemente;
* Configurazioni di sistema e info sui vendor: le configurazioni di rete dei dispositivi connessi devono essere documentate in modo da facilitare il ripristino (switch, bridge, hub). Per avere hw e sw pronto per il ripristino, le info sui venditori devono essere disponibili sul piano;
* Coordinare con polizze di sicurezza e controlli di sicurezza: le soluzioni di contingenza per la LAN dovrebbero essere coordinate con le polizze di sicurezza per proteggere contro minacce che potrebbero interrompere la rete. Inoltre i controlli di sicurezza devono essere implementati per evitare che vengano persi dati sensibili durante l’esecuzione di soluzioni di contingenza;
* Usare i risultati della BIA: per determinare le priorità di ripristino della LAN.

Soluzioni di contingenza

Quando si sviluppa la pianificazione d’emergenza della LAN, il CPC dovrebbe identificare i single point of failure che infieriscono sui sistemi critici o sui processi delineati sulla BIA. L’analisi include minacce al sistema cablato, come tagli, interferenze radio, danni da acqua, fiamme e di altro tipo. Una soluzione è utilizzare cavi ridondati quando lo si ritiene appropriato. Non dovrebbe essere costoso installare duplici cavi per le postazioni di lavoro, mentre lo sarebbe duplicare i cavi in fibra ad alta velocità tra due piani.

Spesso non è costoso duplicare cavi sui vari computer, infatti di solito hanno più porte LAN. Quando i cavi sono installati, un’organizzazione può scegliere di installare extra phone jack ogni alcuni drop. Se si verifica un problema durante l’esecuzione di un cavo, a poca distanza sarà disponibile un cavo funzionante. Un cavo temporaneo può essere utilizzato per raggiungere il jack extra finché il jack problematico non viene sistemato.

Devono essere inoltre considerati nella pianificazione d’emergenza i dispositivi di rete come hub, switch, router e bridge. La BIA dovrebbe identificare il ruolo di ogni dispositivo nella rete, e una soluzione di contingenza dovrebbe essere sviluppata per ogni dispositivo basandosi sulla BIA. Una tecnica è duplicare i router in modo che se uno non funziona più, tutto il traffico viene distribuito sull’altro.

Remote access

È un servizio offerto dai server e dai dispositivi della LAN. Permette la comunicazione tra server e dispositivi disposti su siti diversi. Può essere condotto in vari modi, tra cui VPN. Se un’emergenza o una seria interruzione di sistema occorrono, l’accesso remoto può portare un importante capacità di contingenza fornendo accesso ai dati per i team di recupero o utenti in un’altra locazione. Se è una strategia utilizzata, deve essere identificata la larghezza di banda che permetta l’applicazione di questa soluzione. Controlli di sicurezza devono essere implementati se la comunicazione contiene dati sensibili.

Wireless LAN

È una soluzione di contingenza efficiente per ripristinare i servizi di rete in seguito ad un’interruzione della LAN cablata. Non richiede l’infrastruttura cablata della normale LAN. Può essere installata velocemente come soluzione temporanea o permanente. Però i dati possono essere intercettati quindi i controlli di sicurezza, come la cifratura, dovrebbero essere implementati se la comunicazione include dati sensibili.

Per ridurre gli effetti dell’interruzione della LAN, software di monitoraggio può essere installato. Viene lanciato un alert se un nodo inizia a fallire o non risponde. Il software permette all’amministratore della LAN di venire a conoscenza del problema prima di tutti gli altri utenti. I sw possono essere configurati per inviare automaticamente una pagina elettronica a personale designato quando dei parametri di sistema falliscono o escono dal range.

Fine

Siccome ogni sistema è differente e univo, il CPC deve valutare il sistema usando i risultati della BIA per determinare non solo quali considerazioni e le soluzioni sono appropriate, ma anche quali considerazioni e soluzioni non presentate sono applicabili.

Usare la tabella a pagina 66 per aiutarsi a scegliere considerazioni e soluzioni.

Decisioni da prendere

Stabilimento di contingency: come predisporre i tre tipi di stabilimenti, questo significa:

* Comprendere quali contratti devono essere fatti con le ditte che affittano i vari stabilimenti;
* Comprendere i contratti con le ditte che permettono il backup off-site; v
* Comprendere i contratti con le ditte che permettono il trasferimento di apparecchiatura e la vendita di apparecchiatura di supporto. Anche con quelle per il trasferimento dei media di backup;
* Capire quali sistemi devono essere recuperati nei vari siti, cold conterrà i meno critici e hot i più critici, questo leggendo la BIA;
* Scrivere i motivi delle scelte fatte, di contratti e tutto.

Sicurezza: secondo me qui si può scrivere moltissimo su come facciamo i backup, sulla loro frequenza, su come vengono ridondati i dischi ecc, però probabilmente sono una sezione a parte che posso fare io.

Procedure operative: da capire per ogni sito:

* Cosa deve essere ripristinato in base al problema occorso;
* Qual è l’obiettivo delle varie procedure di ripristino;
* Capire quali team sono coinvolti nel ripristino del sistema nei vari siti;
* Per ogni sito e per ogni team scrivere una procedura di ripristino che rispecchi le soluzioni e le considerazioni viste nella guida;
* Leggendo la BIA bisogna capire l’ordine delle criticità, le procedure vanno in ordine di criticità e anche i vari step di ogni procedura.

Scaletta

Cosa mettere nei vari stabilimenti? Per ogni sito fare una sottosezione di valutazione del costo e della distanza dal sito principale.

1. Cold: risorse per il ripristino di sistemi con bassa priorità di ripristino (nel caso Ican si predisporranno dei backup per i dati dell’applicazione che permette il collegamento con SISS e dovrà essere predisposto un server che permetta l’hosting di tale applicazione, inoltre l’applicazione stessa sarà backupata su un server i cui dati devono essere ridondati); Specificare i vari contratti con vendor di affitto e di trasporto di dati e server per ogni tipo di sito. Siccome i servizi sono in rete, valutare per il ripristino della rete delle vpn che puntino ai server funzionanti sul sito primario;
2. Warm: risorse per il ripristino di sistemi con media priorità di ripristino;
3. Hot: risorse per il ripristino di sistemi con bassa priorità di ripristino; per questo sito specificare che è esterno e che quindi viene fatto un contratto con un’azienda che affitta tutto il sito. N.B. È possibile che più sistemi vengano attivati contemporaneamente a seconda del tipo di danno, ad esempio un danno potrebbe compromettere fattori critici e non critici ma comunque ripristinabili.

I backup sono una sezione a parte, il dove metterli e con quale frequenza, perché non c’entra sullo stabilimento. Vengono backupati i dati dei seguenti server… nel seguente modo… (tipologia di backup), questo per server e pc desktop. Valutare se il servizio interrotto si trova in una specifica area dell’ospedale. In questo caso si può capire quali postazioni di lavoro recuperare.

Possibilità di fare una sezione di premessa dove metti i controlli preventivi:

* Frequenza e tipologia di backup;
* Se si usano raid ups e cose del genere;
* Standardizzare hw e sw e le configurazioni di tutte le postazioni e tutti i server per facilitare il rispristino del sistema.
* Scrivere in questa sezione anche quanto presentato nella sezione dei controlli preventivi della guida.

Le procedure di ripristino vanno fatte così per ogni sito:

1. Selezionare il team che deve eseguire il ripristino e stilare una sequenza di ripristino a step per il team. Questo per ogni team. Esempio LAN recovery:
   1. Farsi spedire il router e il resto dell’apprarecchiatura;
   2. Collegare il tutto;
   3. Installare il sw necessario;
   4. Testare il tutto;
   5. Controlli di sicurezza;
   6. Informare il team leader.
2. Specificare lo scopo della procedura e quindi cosa si intende ripristinare; la sequenza della procedura specifica solo il come si intende ripristinare.

Considerazioni su sicurezza

Postazioni di lavoro

Bisogna inoltre considerare l’utilizzo di chiavi di cifratura nelle strategie di backup. Se queste chiavi vengono memorizzate nel PC, i dati possono diventare non recuperabili se il PC viene corrotto.

Poiché i portatili possono essere rubati, la cifratura deve essere utilizzata per proteggere i dati su un pc rubato. È possibile fornire un secondo disco per quando si esce con il pc, con le minime applicazioni utili a lavorare, in modo che in caso venga rubato, la perdita di dati sensibili è minima.

Server