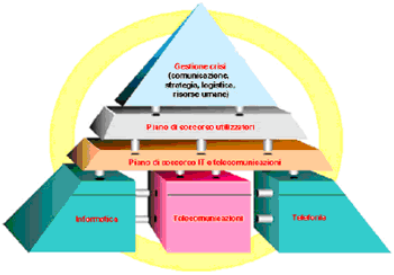
Il Business Continuity Plan

1. DEFINIZIONE



Insieme di soluzioni e procedure che permettono di garantire la continuità dell'attività in caso di sinistro.

2. I PRINCIPI CARDINE

La Sicurezza e la Business Continuity costituiscono una questione di competenza dell'Alta Direzione in quanto richiedono di saper conciliare l'efficacia delle misure di mitigazione dei rischi con l'ottimizzazione delle risorse utilizzate.

Business Continuity Plan significa redigere un piano con la finalità di permettere all'organizzazione di continuare le operazioni necessarie al mantenimento o all'accrescimento del proprio business in qualsiasi condizione critica. Un progetto di questo genere comprende una ristrutturazione ed ampliamento di tutte le procedure interne, una valutazione dei sistemi aziendali (applicazioni, infrastrutture tecnologiche, assetto organizzativo) e un fase di adeguamento e formazione del personale.

Business Continuity Plan (BCP) è il termine utilizzato per indicare le attività finalizzate a garantire il proseguo del business dell'azienda a fronte di eventi classificati, ovvero l'insieme delle attività volte a garantire la continuità dei processi aziendali che concorrono al "core business" dell'azienda. Vengono quindi coperti anche quegli aspetti non prettamente informatici, quali, per esempio risorse umane, interfacciamento verso i fornitori, aspetti comunicativi in caso di crisi.
Questo piano consente di predisporre quanto necessario per:
1. Reagire per assicurare il ripristino dei processi critici
2. Guidare le scelte in caso di crisi
3. Definire procedure alternative per assicurare l'operatività
4. Ridurre il tempo di interruzione dei processi aziendali critici
5. Assicurare che le procedure di ripristino siano efficaci

Tale documento deve possedere una portata operativa immediata. In sostanza, un Business Continuity Plan efficace si basa sull'accettare come fatto che esiste sempre un elemento di rischio: il punto è localizzarlo, valutarlo, stimarne gli effetti e decidere se e come assumersi il rischio. Tutto ciò che è necessario per la continuità operativa, sia i processi essenziali, sia quelli di supporto, devono essere analizzati e presi in considerazione nella definizione di un piano di continuità. Considerando che lo scenario competitivo che influenza la consistenza del business muta continuamente per effetto di fattori esogeni (reazione a cambiamenti del mercato) ed endogeni (riassetto organizzativo) il piano di continuità può essere paragonato ad una istantanea dell'azienda e pertanto valido fino a quando i suoi elementi portanti non mutano. Da

quanto detto si deduce che sicuramente la definizione di un piano di continuità parte da una esigenza di affidabilità dei sistemi intesa non solo come risposta a problemi IT ma soprattutto come Disponibilità dei sistemi a supporto dei Processi di Business.

I confini tematici e metodologici del "Business Continuity Plan" hanno subito negli ultimi anni un significativo mutamento, muovendosi da un'interpretazione rivolta essenzialmente al Disaster Recovery, focalizzato univocamente su information technology and system recovery, a tutti gli aspetti del business spaziando, quindi, dai metodi di alta affidabilità dei sistemi, fino alle gestione delle risorse umane: si è maturata nel tempo la coscienza di essere di fronte ad un processo di gestione che deve essere costantemente revisionato, aggiornato e testato al fine di creare massima aderenza alle esigenze di business (in figura 1 si vede come il Disaster Recovey è una disciplina le cui tematiche sono un sottoinsieme di quelle del Business Continuity Plan.).

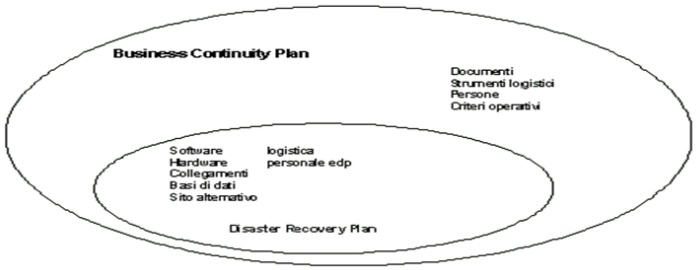


Figura 1 - Business Continuity Plan: un sovrainsieme del disaster recovery

L'obiettivo del Disaster Recovery è quello di garantire a fronte degli eventi classificati, il Ripristino del sistema informatico. La relazione di appartenenza di un Disaster Recovery Plan al dominio del Business Continuity Plan può essere rappresentata nel modo seguente:

3. BCP COME FATTORE CRITICO DI SUCCESSO

Il successo nella progettazione ed implementazione di un Business Continuity Plan efficace è dipendente da un insieme di fattori tra loro collegati:

- Tempo
- Aggiornamento continuo delle soluzioni
- Valutazione continua del rapporto fra costo/complessità della soluzione e valore/priorità

business e normativa del processo protetto
- Costi complessivi
- Ampiezza dell'impatto fra le funzioni coinvolte (in numero e in impegno di risorse)

Una soluzione di Business Continuity è inutile se non è aggiornata ed è sufficiente una variazione ad una qualunque componente del processo alla base per introdurre un elemento di debolezza che può essere determinante. La velocità dei cambiamenti nelle organizzazioni moderne, unitamente all'evoluzione dei mercati, della clientela e della tecnologia è tale che starne al passo costituisce il maggior elemento di criticità dell'intero progetto.
La gradualità nella soluzione, sia in termini di numero di processi considerati che di profondità e dettaglio dell'analisi, è l'unico modo con il quale ridurre la complessità ad una dimensione gestibile ed efficace mantenendo un controllo dei costi. L'aumento tout-court del numero di risorse dedicate (sia interne, che esterne) e del budget economico ha un andamento inferiore rispetto al volume di soluzioni prodotte, in quanto la fruibilità delle soluzioni (condizione necessaria per essere effettivamente tale) rischierebbe di scontrarsi con una struttura non pronta a recepirle e ad attuarle in caso di necessità.

4. LA COSTRUZIONE DI UN BCP

4.1. OBIETTIVI, METOLOGIA E MODELLI

Gli obiettivi portanti di un Business Continuity Plan sono:

- Ripristinare una situazione di normalità, entro un tempo prestabilito, in funzione dei livelli attesi di servizio e di rendere minime le perdite procurate dall'interruzione delle attività.
- Garantire continuità dei principali processi per assicurare l'erogazione dei servizi critici.
  L'implementazione di Continuity Plan pur differendo a seconda dell'ambiente di riferimento, presenta alcuni punti in comune.

E' necessario adottare allora una metodologia di BCP ben strutturata e verificabile; al momento sono disponibili un elevato numero di standard: i più importanti sono quelli sviluppati da:

- Disaster Recovery International Institute" (DRI),
- Business Continuity Institute" (BCI),
- National Institute of Standards and Technology" (NIST)
- Information Systems Audit and Control Association" (ISACA).

Tutte queste organizzazioni concordano sulla presenza del seguente set minimo di best practices quando si disegna e realizza un piano di business continuity:

- deve essere approvato un budget per il BCP da parte del top management;
- deve essere identificato una struttura che in caso di disastro o di interruzione del servizio coordini la strategia di ripristino;
- deve essere previsto un sistema per la gestione degli incidenti o comunque un processo per

controllare la situazione ed operare il ripristino;
- il piano deve essere periodicamente rivisto.

Gli step imprescindibili per implementare un BCP sono:
1. Assessment. Valutazione dei processi aziendali primari e di supporto che evidenzi i processi critici per il core business del cliente e per assicurare un reale coinvolgimento del top management.
2. Analisi dei risultati dell'assesment per definire il perimetro d'azione del L'identificazione del perimetro riveste un ruolo essenziale del progetto. I fattori da considerare sono molteplici:

- Perimetro geografico : N° siti (utilizzatori, tecnici) e locazione.
- Perimetro funzionale : attività interessate dal BCP (es: attività clienti,contabilità....)
- Perimetro tecnico : ambiente informatico
- N° di persone per perimetro geografico/funzionale
- Eventuali date e scadenze.

3. Predisposizione delle procedure da effettuare in caso di attuazione del piano di Business Continuity. Il BCP prevede l'utilizzo delle procedure anche in caso di disastro parziale (indisponibilità di un sottoinsieme dei servizi di infrastruttura) per garantire una reale continuità del business .
4. Supporto post-implementazione. Lo stesso BCP deve prevedere i tempi, le applicazioni da testare e le risorse coinvolte e simulare gli scenari di rischio descritti per singolo processo per verificare la validità delle soluzioni individuate. Inoltre aggiornare le procedure o il piano stesso con le eventuali azioni correttive dedotte dai risultati delle simulazioni.

Il Business Continuity Institute (BCI), in particolare, fornisce una guida operativa che approfondisce soprattutto gli aspetti collegati alla strategia che è alla base della definizione dei fattori critici di successo (a livello di processo e prodotto/servizio) del business.

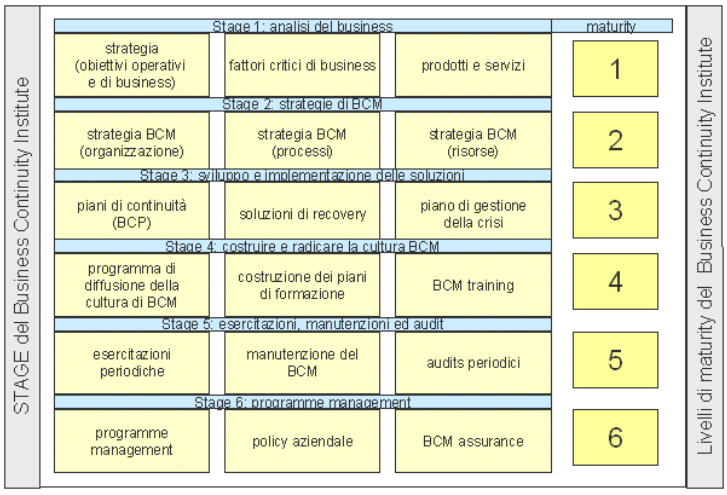


Figura 2 - L'approccio del Business Continuity Institute

Il modello è a carattere generale, non è basato su specifici aspetti tecnici e considera gli elementi della strategia come elementi complessi formati da risorse, organizzazione e processi. L'elemento "sistemi informativi ed informatici" è pertanto una componente del

sistema, nella cui misura del rischio e determinazione delle soluzioni verranno impiegate le linee guida della ISO 27001, mentre per quanto riguarda i modelli di controllo, valutazione e confronti con le best practices vengono seguiti i criteri del **Cobit**.

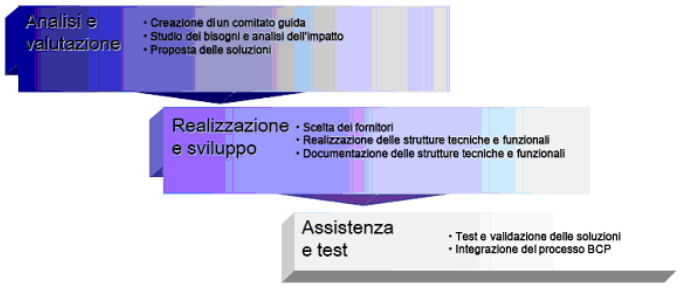
Un'altra strada efficace è quella suggerita dall'**ADFOR**, che suggerisce di suddividere le fasi del modello del **Business Continuity Institute** in 3 gruppi logici:
1. IMPLEMENTATIONE: che comprende i livelli di maturity da 1 a 3, che rappresentano gli stadi iniziali dell'analisi e della progettazione delle soluzioni.
2. SVILUPPO, che equivale al livello individuato dalla maturity 4;
3. MANUTENZIONE, che comprende i livelli 5 e 6.

Ognuno di tali gruppi logici può essere utilizzato come riferimento per un approccio graduale per l'introduzione del BCP in un'organizzazione. Ciò consente di ottenere 4 vantaggi:
1. Si mantiene l'approccio evolutivo step-by-step coerente con il modello complessivo;
2. Si divide e si riduce ulteriormente la complessità frazionando l'approccio e non solo il set di processi;
3. Si garantisce la possibilità di riassemblare via via il lavoro svolto riconducendolo allo standard di riferimento con il minimo sforzo;
4. Si portano in deployment ed maintenance non appena possibile le soluzioni individuate;

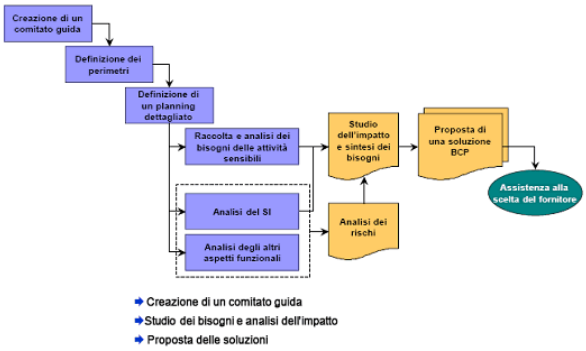
Operando di volta in volta soltanto su una parte dell'intero set dei processi di business, finchè tutti i processi individuati non avranno raggiunto un certo livello di maturity non sarà possibile affermare che il proprio Business Continuity Plan ha raggiunto tale livello di maturity.

4.2. LA METOLOGIA NEL DETTAGLIO

Il seguente schema fornisce una valida guideline per l'implementazione di un BCP.

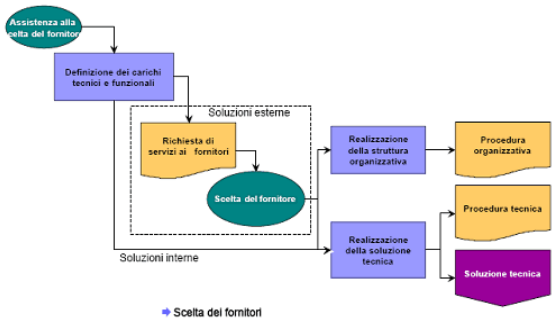


Prima fase : analisi e valutazione



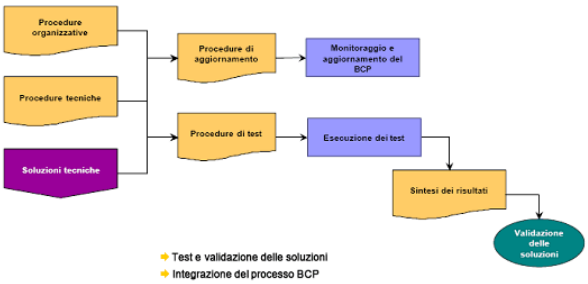
- Creazione di un comitato guida
- Studio dei bisogni e analisi dell'impatto
- Proposta delle soluzioni

Seconda fase : realizzazione e sviluppo



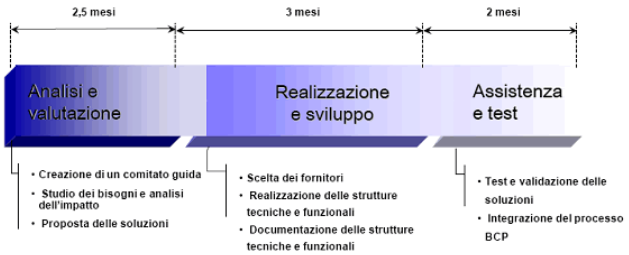
- Scelta dei fornitori
- Realizzazione delle strutture tecniche e funzionali
- Documentazione delle strutture tecniche e funzionali

Terza fase : assistenza e test



- Test e validazione delle soluzioni
- Integrazione del processo BCP

Le tempistiche



4.3 LA MAPPATURA DEI PROCRESSI E DEI LIVELLI DI SERVIZIO PER PREDISPORRE IL BCP

Qualunque sia la realtà che si vuole analizzare, esiste sempre e comunque un punto di partenza: la definizione dei processi e i relativi livelli di servizio.
Nella costruzione di un BCP non si può pensare di limitare l'identificazione dei processi a quelli dell'infrastruttura tecnologica: le tecnologie costituiscono solamente uno degli aspetti che influenzano il corretto funzionamento di un processo. Essenzialmente il punto di partenza è l'identificazione delle esigenze di business: quali strumenti vengono utilizzati dai responsabili dell'organizzazione? Chi sono i process owner? Esiste una procedura che deve essere seguita per svolgere tale attività?. Nel caso in cui esista un sistema informativo di supporto alle attività, come ad esempio un ERP interno all'azienda, è essenziale verificare quali siano i componenti applicativi che forniscono il sevizio; in questo caso specifico la maggior parte degli sforzi per la definizione del piano, devono essere incentrati nell'analisi dell'applicativo: poiché ci si appoggia su un sistema informativo per la totalità o comunque buona parte delle attività, è chiaro che il sistema rappresenta il fulcro del business. Spesso la determinazione di un livello garantito è percepita semplicemente come un contratto attivabile laddove si instauri un rapporto con un fornitore esterno, ma meno ritenuto necessario/opportuno qualora ci si muova nell'ambito aziendale. In una logica di massimizzazione dell'efficienza e dell'efficacia appare auspicabile la sistematica applicazione di regole e presidi analoghi a quelli utilizzati nei rapporti con fornitori esterni. In generale, comunque, l'importanza di fissare con precisione la qualità attesa/garantita dei servizi informatici, di disporre di adeguati strumenti per la sua verifica e di un apposito flusso informativo che renda conto all'utente della qualità effettivamente erogata non sembrerebbe essere un dato acquisito in maniera generalizzata.
Nella definizione dei livelli di servizio è necessario tener conto dell'influenza di più attori coinvolti nella fruizione del servizio. Si prenda a ad esempio un sistema applicativo, le figure interessate sono:

1. Contraente: chi trae vantaggio dall'erogazione del servizio. Definisce tutti i requisiti;
2. Utente: chi utilizza il servizio;
3. Fornitore: chi gestisce il servizio.

Il livello di servizio associato a ciascun processo si ripercuote su ciascun componente applicativo: garantire un livello di servizio per l'intero processo, significa garantire il livello di servizio di ciascun componente.

Una volta identificati i processi più critici e associatogli un livello di servizio, è necessario definire le procedure: come abbiamo detto all'inizio dell'articolo, il Continuity Paln si concretizza in un'insieme di procedure atte a garantire il ripristino dei servizi in caso di "rotture". Che tipo di procedure devo avere? Cosa devono contenere queste procedure?
La definizione delle procedure è differente a seconda della realtà in cui ci troviamo. Risulta pertanto più utile identificare categorie di procedure. Possiamo innanzitutto identificare due differenti categorie:

Generiche: procedure di carattere generale che costituiscono il punto di partenza nella gestione dei problemi. Fanno parte di questo gruppo:

- Procedure di Problem escalation.
- Procedure di Problem determination.
- Procedure di gestione/manutenzione degli ambienti.

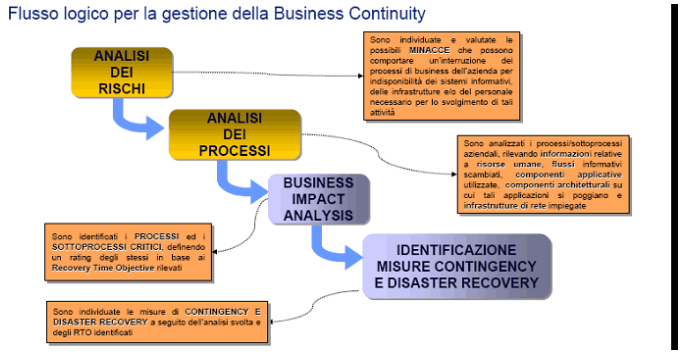
Le procedure di Problem Escalation identificano "le responsabilità" del problema e indirizzano verso l'ente di competenza: ad esempio definiscono i passi necessari per verificare, in caso di fermo di un servizio, se si tratta di un problema sistemistica oppure applicativo. In realtà complesse e dovutamente strutturate (la mancanza di organizzazione interna, è sicuramente l'ostacolo maggiore a cui si incorre nella definizione di un Continuity Plan e per tanto deve essere considerato un prerequisito) le responsabilità e quindi le conoscenze, sono sempre suddivise per enti interni a cui spetta la risoluzione dello specifico problema. Capire l'essenzialità di tali procedure è il punto di partenza per la definizione di un Continuità Plan.

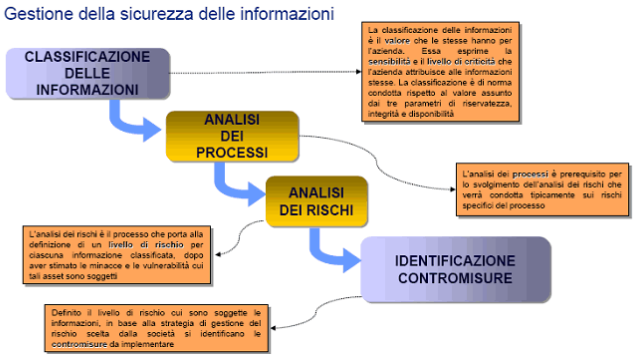
Le procedure di Problem Determination definiscono, una volta affidata la risoluzione del problema ad un ente, gli step necessari per identificare con esattezza il problema. Se esempio se il problema è imputato all'ente sistemi, è suo compito identificare con esattezza la tipologia di problema. Le procedure di Problem determination devono assolvere tale compito.

Le procedure di gestione/manutenzione degli ambienti sono necessarie per il mantenimento dei sistemi e come attività preventiva nei confronti di possibili malfunzionamenti. Tali procedure regolarizzano tutte quelle attività (es. aggiornamenti dei sistemi, installazioni di patch, migrazione degli ambienti, etc.) di "quotidiana" amministrazione che se condotte in modo non "standardizzato" possono condurre a fermi dei sistemi.

5. BUSINESS CONTINUITY PLAN (BCP) E SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI (SGSI)

Le seguenti figure riassumono i milestone fondamentali per la gestione del BCP e del SGSI





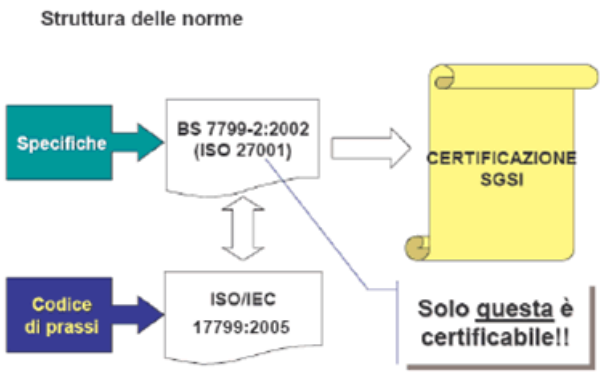
Nel business, avere le informazioni giuste al momento giusto, può fare la differenza tra profitto e perdite. La gestione della Sicurezza delle informazioni aiuta a controllare e proteggere le informazioni aziendali da modifiche volontarie o involontarie dei dati o da accessi non autorizzati.

Un SGSI (Sistema di Gestione per la Sicurezza delle Informazioni), implementato ai sensi degli standard internazionali ISO 27001 ed ISO 17799 serve a:

- assicurare la continuità del business e dei servizi,
- minimizzare i danni derivanti da eventuali incidenti,
- massimizzare:

    a) il rendimento del capitale investito
    b) le opportunità di miglioramento

La sicurezza delle informazioni è, quindi, una responsabilità gestionale, e non un fattore esclusivamente tecnologico. La tutela dei dati personali e delle informazioni di business (know-how) è una priorità in tutti i settori di attività. Gli organismi normatori nazionali ed internazionali hanno emanato disposizioni per ridurre il fattore di rischio legato alla gestione delle informazioni, ad esempio, il nuovo Codice sulla Privacy, o la nuova versione del Trattato di Basilea, che hanno implicazioni per tutti i settori (finanza, manifatturiero, servizi, PP.AA.).
Con gli standard internazionali ISO 27001 ed ISO 17799, le organizzazioni hanno la possibilità di affrontare la gestione delle informazioni ed il tema della loro sicurezza in modo organico, considerando tutti gli elementi che possono avere impatti (risorse umane, processi operativi, sistemi tecnologici, eventi interni ed esterni), focalizzandosi sugli aspetti gestionali.



I 3 aspetti fondamentali della sicurezza delle informazioni sono:

- Riservatezza (o confidenzialità): le informazioni devono poter essere accessibili solo da persone identificate e autorizzate.

- Integrità: i dati e le informazioni devono essere protette da modifiche non autorizzate.

- Disponibilità: i sistemi e le applicazioni devono essere disponibili, quando necessario. Essi vengono valutati e gestiti secondo un classico schema di gestione del rischio.

Ma quali informazioni devono essere protette?

Devono essere protette tutte le informazioni sensibili, critiche o aventi valore per l'azienda ed i suoi stakeholders (clienti, fornitori, personale, comunità, ecc.), in qualsiasi forma si trovino: su carta, in formato elettronico (su sistemi locali, mobili, CD, nastri, etc.), trasmesse via posta o per via elettronica (anche fax), immagazzinate su nastri e video, trasmesse oralmente.

Il SGSI, implementato ai sensi delle norme sopraccitato, è in grado di proteggere le informazioni suddette, perché prevede 4 tipi di controlli;
1) Deterrenti: hanno lo scopo di ridurre la probabilità di attacchi volontari.
2) Preventivi: proteggono le vulnerabilità e rendono gli attacchi inefficaci o ne riducono l'impatto.
3) Correttivi: riducono gli effetti degli attacchi.
4) Investigativi: hanno lo scopo di scoprire gli attacchi e di attivare i controlli preventivi e correttivi.

Occorre fornire le direttive di gestione ed il supporto per le informazioni di sicurezza.

A differenza di sistemi analoghi (ISO 14001; OHSAS 18001) è prevista la redazione di una Dichiarazione di Applicabilità, dove l'Organizzazione rende evidenti i controlli e gli obiettivi per la sicurezza attuati.

6. CONCLUSIONI

Un Continuity Plan essendo uno "strumento" essenziale per garantire piena disponibilità dei servizi, necessita di un po' di tempo e di risorse per poter essere definito; Tutta l'azienda è direttamente coinvolta per lo sviluppo e l'effettivo successo del piano e una cultura di responsabilizzazione della completa struttura aziendale è necessaria come requisito primario.

II fattori chiave del successo di un BCP sono:

- Partecipazione del management al comitato guida
- Garantisce la fluidità del progetto.
- Le decisioni prese hanno peso per i responsabili attività.
- Un referente unico presso il cliente
- Consente di centralizzare richieste e informazioni.
- Gestisce gli eventuali conflitti.
- Collaborazione con i consulenti esterni
- Consente l'implicazione dei consulenti esterni nel progetto.
- Garantisce l'identificazione dei bisogni e la loro integrazione nella pianificazione.
- Sensibilità alle scadenze
- Consente la disponibilità dei mezzi necessari al raggiungimento degli obiettivi nei tempi stabiliti.

FONTI:
http://www.mokabyte.it/
http://www.clusit.it/smau_roma_2002/presentazione_bcp_smau_blanco2.pdf
http://www.lra.it/web/dettaglioNews.do?newsId=3825
http://www.adfor.it/consulting/businesscManagement.asp
http://apache.tecnoteca.it/upgradepdf/it-up46Grillo.pdf#search=%22business%20continuity%20plan%22