MASTER UNIVERSITARIO di II Livello

in

HOMELAND SECURITY

Università Campus Bio-Medico – Roma

Consorzio NITEL

Anno accademico 2013/2014

PROJECT WORK ABSTRACT

Business Continuity: Linee Guida per le PMI

Relatore: Dott. Alessandro Senatra

Tutor: Dott. Alessandro La Daga

Abstract

Il presente projectwork nasce dalla cooperazione tra Quality Solutions e BCManager con il fine di realizzare, per la prima volta in Italia, uno studio di settore sullo stato dell'arte della BC e dei BC manager nelle diverse aziende italiane. La scelta dell'argomento per la stesura dell'elaborato finale, come lavoro di fine percorso formativo, è stata fatta con l'interesse sorto nel coinvolgimento operativo e il supporto fornito dal candidato. Tale projecwork si pone il fine di fornire una panoramica, volutamente non tecnica, sulla BC al fine di poter essere compresa e utilizzata come linea guida dalle PMI italiane.

Dopo un introduzione sulla Business Continuity a spiegazione dell'importanza della materia, la seconda parte prende in esame i concetti di *Business Impact Analysis* e *Risk Assessment*, illustrando sinteticamente la metodologia: in particolare si è dato molto risalto alla fase di analisi.

Esistono molte PMI o grandi imprese che non sono adeguatamente preparate alla gestione di incidenti potenzialmente disastrosi, ovvero incidenti che potrebbero causare l'interruzione del business o parti di esso per periodi limitati o lunghi[1]: ciò è dovuto all'assenza o al mancato aggiornamento di un Business Continuity Plan (BCP).

[1] Si vuole precisare che il tempo nella BC non è un valore di riferimento assoluto. La componente temporale nella BC può essere scorporata in due variabili. La prima riguarda la validità nel tempo dei piano di BC. La seconda concerne la durata dell'interruzione.

La mancata preparazione delle organizzazioni può comportare perdite significative, sia sul piano finanziario sia sul piano economico[2]. Un determinato evento disastroso può colpire sia un'organizzazione sia un intero settore industriale. Ne sono un esempio il settore dei trasporti aerei, nel quale in seguito agli attentanti del 2001 le compagnie aeree subirono ingenti danni finanziari ed economici, e l'industria della pesca nei paesi del sud-est asiatico in seguito allo *tzunami* del 2004[3].

Le organizzazioni dovrebbero essere in grado di sopravvivere e continuare le loro attività anche dopo un evento disastroso. Per questo è necessario sviluppare nella cultura aziendale una "*forma mentis*" che permetta di analizzare, identificare e gestire tutti i rischi che possano esporre l'organizzazione a danni derivanti dalla:

- Incapacità di adempiere a obblighi normativi o contrattuali
- Mancata protezione degli *asset* aziendali
- Incapacità di erogare servizi o consegnare prodotti ai proprio clienti
- Perdita del valore del marchio, dell'immagine e della reputazione

Per questi motivi il *Business Continuity Management* costituisce un elemento essenziale per assicurare la sopravvivenza dell'organizzazione.

Il primo strumento metodologico presentato è la *Business Impact Analysis* che ha lo scopo di fornire una stima di danni quantitativi in funzione del tempo

[2] Nelle perdite economiche possono rientrare il brand e le future commesse

[3] Ogni tipologia di business o settore industriale è esposto ad eventi diversi i quali possono causare diverse tipologie di danni come la perdita dei clienti, dei profitti, della reputazione, delle licenze governative e così via.

d'interruzione di un processo o servizio dell'organizzazione. Affianco alla quantificazione dei danni diretti e indiretti si indentificano gli impatti di perdita d'immagine, reputazione, brand, conseguenze amministrative e/o "penali"[4]. Attraverso la stima degli impatti si possono fissare gli obiettivi di ripartenza (RTO[5]) da rispettare affinché l'organizzazione possa contenere i danni.

Il secondo strumento metodologico presentato è il *Risk Assessment*, finalizzato a comprendere l'esposizione di un processo rispetto a determinati *Risk Scenarios*.

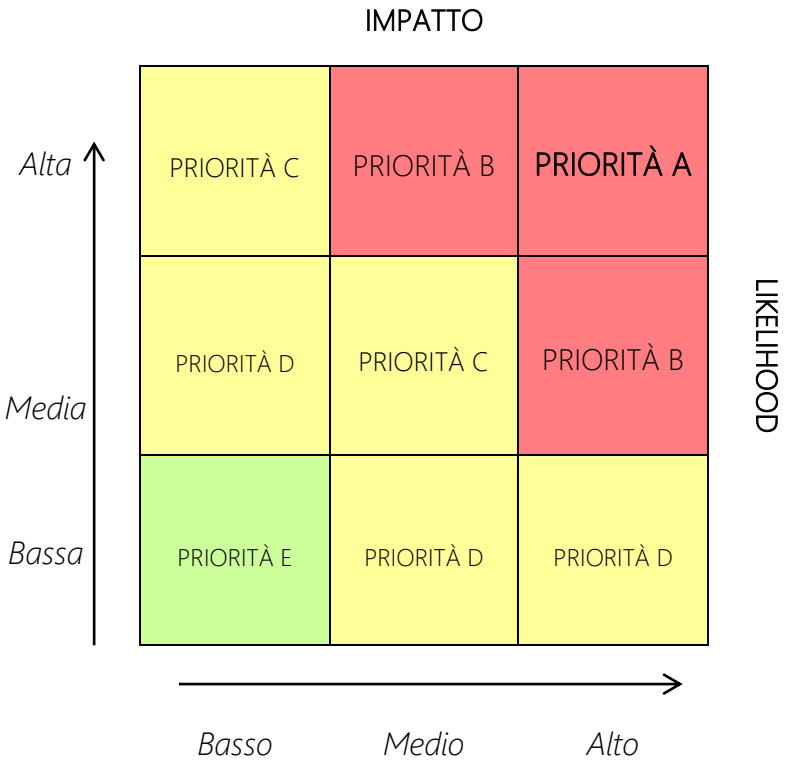
Al fine di quantificare il rischio si dovrà calcolare un indice che considera, oltre agli Impatti e alla Probabilità, anche le Vulnerabilità, specificamente legate al livello di adeguatezza delle misure tecnico-organizzative di prevenzione/reazione. La formula utilizzata per il calcolo del *Risk Profile* è:

$$Rischio = Impatto \times (Probabilità \times Vulnarabilità)$$

L'impatto può essere visto come la componente del rischio che permette di comprendere la dipendenza dei processi rispetto alle risorse (risorse umane, sistemi informativi, spazi di lavoro, servizi infrastrutturali e *supply chain*). La probabilità, rappresenta la frequenza di accadimento di un evento specifico (es. terremoto, fallimento fornitori, blackout, attacchi informatici…) e la vulnerabilità, rappresenta la sensibilità o l'esposizione della risorsa alla minaccia. L'insieme dei *Risk Profile* derivanti dalla valutazione degli scenari può essere rappresentato su

[4] La violazione o l'inadempienza di obblighi di legge o contrattuali può comportare, oltre a impatti qualitativi (predita della licenza, procedimenti amministrativi/penali/tributari…) anche danni finanziari diretti (panali, sanzioni) e indiretti (lucro cessante).
[5] Recovery Time Objective

una matrice che combina la ***likelihood*** (probabilità x vulnerabilità) e l'impatto (dipendenza) sul processo in caso di indisponibilità di una delle risorse.



Una buona strategia di *Business Continuity* serve a gestire il rischio associato ai casi in cui un processo sia fortemente dipendente da una risorsa specifica (priorità "a" e "b"). In ottica di miglioramento continuo è possibile ottimizzare gli investimenti intervenendo prioritariamente su una parte dei rischi, implementando delle soluzioni per mitigare il rischio e pianificando le modalità operative gestione della crisi e del ripristino dei processi.