Business Continuity Plan, questo sconosciuto

Il BCP (*Business Continuity Plan*) o **Piano di Continuità Operativa** è un documento richiesto alle **organizzazioni certificate ISO 27001** (*Sistema di gestione per la sicurezza delle informazioni* – Requisiti) al controllo A.17.1 "Continuità della sicurezza delle informazioni", ma anche – e soprattutto – dalla norma specifica UNI EN ISO 22301:2014 – *Sicurezza della società – Sistemi di gestione della continuità operativa – Requisiti*, che abbiamo trattato in un precedente articolo.

Gli eventi delle ultime settimane, ma anche degli ultimi anni, hanno mostrato quanto scarsa sia l'adozione di questo strumento nel nostro Paese. Molti sono, infatti, gli esempi di situazioni critiche – essenzialmente causate da disastri naturali – che non sono state fronteggiate nel modo corretto e che hanno portato a costi sociali elevatissimi che si sono scaricati inevitabilmente sulla collettività:

- Il terremoto dell'Aquila e dell'Emilia;
- Le alluvioni in Liguria ed in Toscana;
- Le interruzioni di energia elettrica protrattesi nel tempo a Cortina qualche Natale fa e, più recentemente, in Emilia dopo una forte nevicata;
- Le forti nevicate verificatesi in Emilia-Romagna nel 2012.

In tutte queste situazioni di emergenza, oltre ai danni materiali ed alle perdite di vite umane, si sono verificate disfunzioni e ritardi nella **ripresa dell'operatività ordinaria**. Il vantaggio di avere predisposto un buon piano di continuità operativo è proprio questo: ipotizzando una situazione di crisi si cerca di **limitare i danni** e di **tornare all'operatività normale nel più breve tempo possibile**.

Tornando ad aspetti più tecnici, mentre la **ISO 27001** tratta la continuità operativa in termini di sicurezza delle informazioni, ovvero di garantire il ritorno alla piena disponibilità delle informazioni senza perdite significative delle stesse, la **ISO 22301** amplia il raggio di azione del *business continuity plan*, comprendendo la gestione delle discontinuità di un servizio, non necessariamente legato alla disponibilità di informazioni su supporto cartaceo o elettronico (anche se oggi ben poche attività possono farne a meno). Alcuni esempi possono chiarire meglio il concetto:

- La gestione di un ospedale a fronte di grandi epidemie che riducono anche la

disponibilità di risorse umane sufficienti ad affrontare l'emergenza;
- Un servizio di trasporto di persone o beni in caso di calamità naturali;
- Un servizio di pronto intervento di manutenzione in caso di calamità naturali che impediscono al personale di recarsi al lavoro;
- Un servizio di ristorazione collettiva in caso di calamità naturali o epidemie influenzali che impediscono al personale di recarsi al lavoro;
- E così via.

Si ricorda che la **continuità operativa** è l'insieme di attività volte a minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che ha colpito un'organizzazione o parte di essa, garantendo la continuità delle attività in generale.

La sfera di interesse della continuità operativa va oltre il solo ambito informatico, interessando l'intera funzionalità di un'organizzazione (Azienda, Ente Pubblico, ecc.) ed è, pertanto, assimilabile all'espressione "*business continuity*".

La continuità operativa comprende sia gli aspetti strettamente organizzativi, logistici e comunicativi che permettono la prosecuzione delle funzionalità di un'organizzazione, sia la continuità tecnologica, che riguarda l'infrastruttura informatica e telecomunicativa (ICT) ed è nota come "*disaster recovery*" (DR). Pertanto, le soluzioni per garantire la continuità dei servizi non considerano soltanto le componenti tecnologiche utilizzate, ma anche tutte le altre risorse (personale, impianti, infrastrutture, ecc.).

Le analisi, valutazioni e scelte di trattamento del rischio richieste dalla gestione della continuità operativa sono le seguenti:

- Identificazione dei rischi;
- Analisi e valutazione dei rischi;
- Analisi delle conseguenze di disastri, malfunzionamenti, interruzioni di servizi (*Business Impact Analysis*);
- Realizzazione di piani (controlli) affinché i processi di business siano riattivati entro il tempo richiesto.

Le analisi valutano per ogni *asset* (o gruppo di *asset*) critico il tempo che tale *asset* può rimanere indisponibile con danno basso o nullo. I piani (*Business Continuity Plan*) devono essere mantenuti costantemente aggiornati per essere efficaci al momento del bisogno.

Per meglio comprendere la predisposizione di un BCP occorre introdurre alcune definizioni basilari:

- **Mission Critical Activity** (MCA): attività critica o di supporto al business relativamente ai servizi o prodotti offerti dall'organizzazione (internamente o esternamente), incluse le sue correlazioni con altri processi e *single points of*

failure, che permettono all'organizzazione di raggiungere i suoi obiettivi di business considerando le stagionalità e/o tempi di rilascio critici
- **Business Impact Analysis** (BIA): analisi gestionale attraverso la quale un'organizzazione valuta quantitativamente (per esempio finanziariamente, *Service Level Agreement*, SLA) e qualitativamente (per esempio reputazione, leggi, regolamenti) gli impatti e le perdite che possono risultare se l'organizzazione subisce un grave incidente, e il minimo livello di risorse necessarie per il ripristino.
- **Maximum Tollerance DownTime** (MTDT): massimo intervallo di tempo ammissibile di interruzione del servizio (*quante ore posso permettermi di non erogare il servizio ai clienti?*).
- **Maximum Tollerance Data Loss** (MTDL): massima perdita di dati tollerata (*quanti dati posso permettermi di perdere?*).
- **RTO** (*Recovery Time Objective*): periodo di tempo entro il quale devono essere ripristinati un minimo livello di servizio, i sistemi di supporto e le funzionalità principali dopo un'interruzione dei servizi. Normalmente è il lasso di tempo entro il quale cui le MCA devono essere ripristinate.
- **RPO** (Recovery Point Objective): istante (punto) nel tempo al quale i dati sono coerenti e possono essere ripristinati.
- **MBCO** (*Minimum Business Continuity Objective*): livello di servizio minimo accettabile dall'organizzazione per raggiungere i propri obiettivi di business durante una rottura.

Il processo di gestione della continuità operativa deve prendere in esame tutti i processi e le attività aziendali e classificarli in funzione della loro criticità nel modo seguente:

1. Attività critiche per il business (MCA's);
2. Attività importanti;
3. Attività secondarie.

Per le **attività critiche** vengono stabiliti degli **obiettivi di continuità operativa** in termini di MTDT, MTDL, RTO, RPO, MBCO e stabiliti dei **piani di continuità operativa**, che comprendono le contromisure messe in campo per garantire gli obiettivi.

Per la pianificazione delle attività di continuità operativa è necessario valutare preliminarmente gli impatti degli eventi che possono causare interruzioni dei processi di business, predisponendo una BIA.

A seguito della **valutazione dei rischi di interruzione del servizio** erogato ai clienti devono essere predisposti, attuati e periodicamente verificati uno o più **Piani di Continuità Operativa** (*Business Continuity Plan*) aventi lo scopo di mantenere o ripristinare il funzionamento dei processi critici ed assicurare la disponibilità delle informazioni necessarie a garantire un **livello di servizio accettabile**, a fronte del verificarsi dei rischi di interruzioni o malfunzionamenti

precedentemente identificati e valutati.

Dunque se pensiamo ad un servizio di pubblica utilità (servizi ospedalieri, trasporto pubblico, mense scolastiche, servizi di pulizia e raccolta rifiuti, ecc.) occorre definire due livelli:

- Un primo livello che identifica il ripristino di un servizio minimo dopo l'interruzione;
- Un secondo livello che sancisce la ripresa dell'attività ordinaria.

Per ogni livello devono essere stabiliti i tempi entro i quali vengono raggiunti e che possono costituire SLA contrattuali.

È bene comprendere che i BCP devono prefigurare uno **scenario di crisi** ben definito, al verificarsi del quale si vuole reagire in modo adeguato. Chiaramente non tutti gli scenari possibili possono essere gestiti nei BCP, ma solo quelli **più probabili e di impatto più grave**, sulla base della valutazione dei rischi preliminarmente svolta.

I contenuti dei BCP potrebbero essere i seguenti:

1. Scopo e campo di applicazione
2. Obiettivi
3. Requisiti di business continuity (RPO, RTO,…)
4. Identificazione dei processi critici (MCA's)
5. *Business Impact Analysis*
6. Piano di *Disaster Recovery*
7. Piano di Continuità Operativa, contenente:

- Rilevazione dell'incidente (metodi e procedure): dichiarazione del disastro o incidente, valutazione del danno, attivazione del piano):
- Risposta all'incidente (attività, tempi, responsabilità, procedure);
- Ripristino dell'operatività (attività, tempi, responsabilità, procedure di azione e continuità);
- Risorse (personale e competenze, tecnologie, infrastruttura, software, dati, siti alternativi, centri di emergenza o crisi);
- Fornitori (Lista dei fornitori di *recovery*, dettagli dei contratti, procedure di attivazione);
- Organizzazione e Responsabilità;

- Documentazione;
- Comunicazioni (contatti, soggetti da informare, messaggi);

1. Test del BCP (prove, tempi, responsabilità)
2. Manutenzione del BCP

Si precisa che i BCP possono far riferimento ad altri documenti (ad es. Piani di *Disaster Recovery*), aggiornati autonomamente. In ogni caso deve essere sempre possibile risalire alla configurazione attuale del BCP, ovvero alle revisioni vigenti dei documenti esterni richiamati nel Piano di Continuità Operativa. Tale configurazione e la relativa rintracciabilità dei documenti relativi al BCP deve essere disponibile sia in formato elettronico, sia su supporto cartaceo, con gestione di copie di riserva del BCP disponibili in locali/siti/ubicazioni alternative, al fine di essere sempre disponibili in caso di verificarsi dell'evento che ha generato l'interruzione dei processi critici.

Si rammenta che per la Pubblica Amministrazione la continuità operativa ed i relativi Piani di Business Continuity sono previsti dall'Art. 50 bis del Codice per l'Amministrazione Digitale; essa, pertanto, deve essere gestita dagli responsabili degli Enti Pubblici in modo adeguato, con riferimento agli standard internazionali sulla materia.

[Download non trovato]