Business Continuity, l'importanza di una sinergia tra le strutture aziendali per una migliore resilienza d'impresa

Articolo a cura di Michele Magni, senior manager Clever Consulting

Continuità operativa e resilienza d'impresa rappresentano due aspetti fondamentali per il business di un'azienda. Oggi più che mai l'avvento delle nuove tecnologie ha reso necessario per le imprese adottare una visione più olistica, identificando in anticipo i potenziali rischi che minacciano l'organizzazione e rispondendo in tempi relativamente brevi a situazioni di crisi. Questo al fine di salvaguardare le attività produttive, gli interessi dei propri stakeholder, la propria immagine e la posizione sul mercato di riferimento.
Soprattutto in ambito tecnologico, il successo e l'efficacia di una strategia di continuità operativa dipendono in buona parte dalla capacità di coinvolgere attivamente tutte le strutture aziendali nel suo processo di gestione, in modo da garantire una migliore resilienza del business.

Ma quali sono i fattori da prendere in considerazione per l'attuazione di un efficace progetto e successivo processo di Business Continuity Management?

Uno dei principali aspetti da tenere presente è sicuramente la **comunicazione**, cioè l'utilizzo di termini comuni e la condivisione dell'ambito di riferimento, per portare l'IT "fuori dall'IT" e fare in modo che le altre strutture aziendali comprendano l'importanza di coinvolgere la tecnologia in tutte le fasi del piano di business continuity. In questo il BCI (Business Continuity Institute) fornisce importanti indicazioni. Non va infatti dimenticato che la gestione della continuità operativa non ha ancora una sua collocazione fissa nell'organigramma aziendale, e che l'utilizzo di approcci e terminologie comuni non è affatto scontato ma dipende dallo specifico contesto aziendale.

Dal momento che il piano di continuità operativa rientra nella politica di gestione dei rischi e tra i più significativi rientrano, direttamente o indirettamente, anche i rischi di natura tecnologica, altro aspetto da considerare è il **risk management**. È quindi vitale condividere le informazioni e ottimizzare l'analisi dei rischi; analisi su cui sempre più si basa non solo il business, ma anche le altre strutture aziendali di supporto. Riuscire a comprendere i rischi IT contribuisce infatti a rendere il risk manager più consapevole delle innumerevoli connessioni che caratterizzano le diverse aree operative dell'azienda.

Mancanza di tempo e priorità sono due elementi che l'IT si trova quotidianamente ad affrontare, rendendo spesso arduo il compito di gestire al meglio le procedure, la documentazione e il tracciamento delle attività legate alla continuità operativa. Da qui la necessità di rispettare tutte le esigenze di **compliance**, per non rischiare di dover far fronte a sanzioni legali e perdite finanziarie che potrebbero ledere la reputazione dell'organizzazione e rallentare i processi aziendali. Per questo motivo è consigliabile sottoporre regolarmente il piano di continuità operativa alla revisione di terze parti che abbiano le giuste competenze in materia.

Di fondamentale importanza sono inoltre le competenze specialistiche che gli addetti ai lavori devono possedere - ad esempio sulle tecnologie di rete, sul database, in ambito middleware, ecc. - sottoponendoli periodicamente ad **aggiornamento professionale**. Solo così saranno in grado di monitorare l'adeguatezza dei sistemi informativi e la loro affidabilità, attraverso criteri di valutazione e controllo efficaci sia in fase di implementazione, sia in fase di mantenimento del piano di Business Continuity.

L'aspetto **sicurezza** è invece trasversale a qualsiasi attività con un impatto anche tecnologico, sia durante il normale svolgimento delle operazioni, sia in situazioni di emergenza. Per esperienza personale, tre sono le tematiche che si riscontrano con maggiore frequenza:

- la gestione in emergenza delle credenziali amministrative (soprattutto nello scenario di indisponibilità delle risorse critiche IT);
- l'eventuale "deroga" alle disposizioni di sicurezza in caso di situazioni straordinarie di emergenza;
- la gestione del cambiamento (Change Management).

Altro aspetto che merita particolare attenzione è quello delle **risorse umane**, fondamentali per l'ottenimento di risultati significativi in relazione al mantenimento della continuità operativa all'interno dell'azienda. In questo caso è necessario agire con interventi formativi sia per i dipendenti, sia per il management, e impostare preventivamente i processi di gestione del personale in caso di effettiva emergenza (inclusi aspetti di mantenimento delle informazioni di contatto, reperibilità, aspetti contrattuali e sindacali, ecc.). La tecnologia può rappresentare un elemento di facilitazione per il raggiungimento degli obiettivi HR, in quanto l'interazione tra comparto HR e IT può supportare la definizione di soluzioni più efficaci ed evolute, anche nell'ottica di incentivare l'applicazione dello "smart working".

Abbiamo infatti notato come l'indisponibilità di personale essenziale per il funzionamento dei processi IT aziendali venga spesso sottovalutato, anche in quei contesti in cui proprio il personale IT dovrebbe essere immediatamente disponibile per garantire i processi di ripristino.

Va infine considerato un altro lato della **comunicazione**, differente da quello citato inizialmente e che spesso rileviamo in situazioni di Crisis Management. All'interno di un piano di continuità operativa è fondamentale definire in anticipo un piano di comunicazione per stabilire con quale frequenza e in quale modo le informazioni devono essere trasmesse nel corso della crisi: verso i dipendenti - che come abbiamo detto vanno preventivamente formati - verso i clienti, le controparti rilevanti, le autorità, i media e tutte le strutture aziendali coinvolte. Anche in questo ambito l'IT riveste un ruolo importante, in quanto la comunicazione in casi di emergenza dipende spesso da soluzioni gestite dallo stesso IT.

Un'azienda che vuole essere resiliente e implementare un piano di Business Continuity di successo, deve quindi prestare attenzione a questa domanda di sinergie tra i diversi ambiti aziendali, che è sempre più in aumento e necessita di una risposta concreta ed effettiva per rendere più organici e sostenibili i progetti di Continuità IT e, più in generale, di Continuità Operativa. Questo processo non è certamente privo di difficoltà, ma il mercato è maturo e le aziende, nelle giuste condizioni, possono e devono considerare e cogliere queste opportunità governando il processo di Business Continuity sotto tutti i punti di vista, non solo quello tecnologico.