Il Business Continuity Plan - Non solo tecnologia, non solo carta

Date : 17 gennaio 2018

6 elementi imprescindibili per un buon piano di continuità

"La Business Continuity? Grazie ma sono a posto, ho il piano di Disaster Recovery!" Ho sentito molte volte questa frase. E ogni volta è stato difficile confutare tale convincimento, provando a chiarire cosa sia veramente la Business Continuity senza far sentire l'interlocutore un ignorante. Alla base di quell'affermazione c'è infatti una grave lacuna teorica e pratica.

Con grande pazienza occorre spiegare che il piano di Disaster Recovery è sì molto importante ma è soltanto una parte dell'intero Sistema di Gestione della Continuità Operativa (Business Continuity Management System) di un'organizzazione.

Il piano di Disaster Recovery rappresenta infatti uno dei piani di livello operativo, al pari del piano di emergenza del sistema elettrico, il piano di evacuazione, il piano logistico per trasportare le persone in un sito alternativo, e di tutti gli altri piani che sono orientati all'azione e che traducono quindi in azioni le decisioni prese precedentemente a livello strategico e tattico. Ma, così come gli altri, è ben lontano dal coprire da solo tutte le esigenze di continuità di un'organizzazione.

Spesso i clienti si rivolgono a noi dicendo: "Ci dicono che dobbiamo avere un piano di continuità operativa. Quanto costa? Quanto tempo ci mettete a scrivermelo?" Siamo contattati regolarmente da organizzazioni che cercano assistenza nell'elaborazione di un piano di continuità operativa.

In certi casi, ci sono aziende – fornitori di terzi – che arrivano a noi perché clienti importanti hanno chiesto loro di dare evidenza di un buon piano di continuità, oppure perché vedono il piano in sé e per sé come l'elemento che da solo li protegge dalla discontinuità operativa. Vogliono quindi ottenere un piano e chiudere così la questione della Business Continuity. SBAGLIATO! La continuità non è un discorso che si risolve con un pezzo di carta caduto dall'alto, e un piano di continuità non è un attestato una tantum che garantisce di per sé la continuità di un'organizzazione.

I piani di Continuità Operativa sono documenti che indicano decisioni e soluzioni a cui l'organizzazione arriva dopo un percorso e che vengono costantemente tenuti in vita da esercitazioni, test e aggiornamenti.

Si inizia analizzando gli impatti e le minacce ai propri processi prioritari, quelli che non vogliamo che si interrompano mai, si effettua un'analisi costi/benefici di tutte le soluzioni e le alternative per garantire la continuità operativa a fronte di gravi interruzioni, e si prendono decisioni relative anche a tutto ciò che in azienda non è considerato urgente. Solo a questo punto è possibile catturare tali strategie di continuità in un piano. Questo iter non è necessariamente lungo e faticoso; se siete o se consultate esperti di Continuità e Resilienza, ve ne renderete conto.

Ovviamente tutto dipende anche dalla natura, dalle dimensioni e dalla complessità di un'organizzazione, ma ci sono degli elementi da cui nessun piano di Business Continuity può prescindere:

1. **Deve rispondere chiaramente alle domande: chi, cosa, dove, come e quando.**

Chi è responsabile, chi è coinvolto? Cosa occorre fare (con chi ci mettiamo in contatto, cosa abbiamo previsto di fare in questo caso, ecc.)? Dove abbiamo spazi alternativi? Come avviene il trasferimento (di informazioni, sistemi, persone, cose o fornitori)? Qual è il limite oltre il quale le risorse a disposizione diventano insufficienti? Questi sono solo alcuni esempi delle domande da porsi; per ottenere le informazioni corrette che alimenteranno il piano, occorre far riflettere tutti gli attori coinvolti nel ripristino del Business.

2. **Deve essere utile da cima a fondo.**

Il documento non deve contenere informazioni irrilevanti. Eliminiamo tutto ciò che non servirebbe durante un evento critico. Nei piani di ogni organizzazione capita di imbattersi in molte informazioni che servono a soddisfare le autorità di regolamentazione, a volte il legale o i sindacati. Mettiamo tutte le informazioni in legalese o politichese in un manuale di continuità e lasciamo che i piani siano utili a chi ne deve usufruire durante un evento critico e non gli facciano perdere tempo a leggere parole vuote. Il miglior piano di continuità è una check list: conciso, diretto e rilevante.

3. **Deve indicare cosa dovranno fare sia coloro per i quali abbiamo studiato soluzioni alternative (titolari di processi critici), sia coloro per i quali non è stata studiata alcuna strategia.**

Il piano tecnologico e il piano logistico devono prepararci ad affrontare il tema del ripristino di tutte le funzioni e il ritorno alla normalità – non solo per i processi critici. Se un'organizzazione si preoccupa di catturare solo le azioni orientate alla tutela dei processi critici, non sarà sufficientemente resiliente. Occorre avere un quadro preciso di quanto si dovrà fare per ridare a tutti un ufficio e la tecnologia che occorre per continuare le attività. È importante quindi ricordare che l'analisi d'impatto riguarda solo i processi critici, mentre i piani di continuità operativa riguardano la totalità dell'organizzazione.

4. **Deve essere elaborato coinvolgendo l’intera unità organizzativa per cui viene scritto.**

Un piano sviluppato da uno per molti è sempre meno efficiente di un piano proposto da uno e condiviso con tutti. Basta poco per proporre le azioni da eseguire durante un evento critico. I responsabili coinvolti, con la propria esperienza e competenza e con il proprio talento e creatività, daranno contributi irraggiungibili da un singolo individuo che, per ovvi motivi, non può essere direttamente coinvolto in tutte le attività.

5. **Deve essere scenario independent.**

Se parliamo di piani di Continuità Operativa generici (ad esempio il piano di crisi o il piano di una singola unità organizzativa), la riflessione che conduce alla scrittura del documento deve sempre essere indipendente da un’ipotesi di scenario (*scenario independent*). Questo perché l’interruzione può avvenire per molteplici ragioni e il piano deve soddisfarle tutte. Come ben indicato dallo standard internazionale di riferimento (BS 11200:2014 - Crisis Management), a prescindere dalla causa (un atto terroristico, una catastrofe naturale o un attacco degli hacker ai nostri sistemi), dobbiamo essere pronti a prendere decisioni velocemente per mitigare i danni e ripartire.

Ci saranno poi i piani di Continuità Operativa specialistici che saranno elaborati con esperti del settore. I tipici piani specialistici sono il piano della comunicazione, il piano per il recupero dei prodotti, il piano per la perdita di dati (data breach, ransomware e data disclosure), il piano pandemico, il piano per i rapimenti e così via.

6. **Deve essere sempre esercitato.**

Ci sono metodi di convalida del piano molto semplici, poco costosi e estremamente efficaci. L’importante è che il piano venga tenuto sempre in vita e sia pronto a essere utilizzato agevolmente in caso di una reale interruzione.

In un contesto in cui le minacce al business crescono e si evolvono giorno per giorno, i piani di continuità sono un elemento fondamentale per il successo a lungo termine di qualsiasi organizzazione. Con tutti questi punti in mente – e se interpellerete esperti che credono veramente in questa disciplina – avrete sicuramente dei risultati positivi sulla resilienza della vostra organizzazione.

A cura di: **Gianna Detoni**