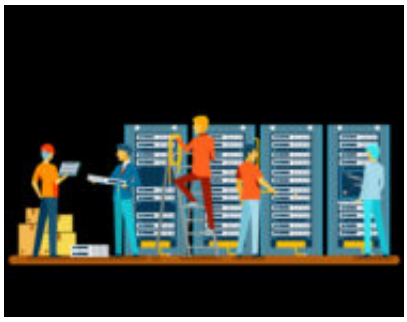
Continuità operativa: le definizioni fondamentali

Date : 28 febbraio 2018



Questo articolo prosegue la serie dedicata a temi su cui ci sono i maggiori dubbi e perplessità sulle norme della serie ISO/IEC 27000.

Qui si affrontano i termini fondamentali relativi alla continuità operativa, spesso oggetto di confusione. Non si forniscono metodi per pianificare e attuare la continuità.

Nulla vieta di usare altri termini, ma è necessario avere conoscenza di quelli di riferimento, anche per assicurare chiarezza nel confronto con altre entità (per esempio, clienti e auditor).

Disaster recovery

Con il termine *Disaster recovery* si intende l'insieme di soluzioni volte a ripristinare i sistemi informatici in caso di loro indisponibilità prolungata.

Il termine è fuorviante perché non include il termine "informatico" e lascia intende che sia utile solo in caso di disastro, mentre lo è anche quando i sistemi primari sono indisponibili, per esempio, a seguito di cambiamenti non corretti o blackout.

Il *sito di disaster recovery* è il luogo dove si prevede siano ripristinati i sistemi informatici e deve essere distinto dal sito cosiddetto *primario*.

Il *piano di disaster recovery* è l'insieme di procedure da seguire per attivare il sito di *disaster recovery*.

Business continuity o continuità operativa

Il termine *business continuity* riguarda i processi di un'organizzazione. Esso li deve considerare tutti e poi selezionare quelli critici (o *urgenti*) per cui prevedere procedure di ripristino dettagliate.

Il *piano di business continuity* (o BCP) è l'insieme di procedure da seguire quando si verifica un incidente che blocca la normale operatività dei processi per un lungo periodo.

Quando si parla di un’azienda che eroga servizi informatici, gran parte del piano di *business continuity* coincide con quello di *disaster recovery*. In altre aziende (per esempio di produzione), il ripristino dei sistemi informatici costituisce una parte del BCP.

Nel caso della *business continuity* non è previsto un termine per indicare il sito dove riprendere le attività non informatiche, anche se sono spesso usati *sito alternativo* o *sito secondario*.

Il *ritorno alla normalità* è l’insieme delle attività necessarie a ripristinare tutti i processi allo stesso livello precedente l’incidente. Non esiste un termine per indicare il periodo tra l’incidente e il ritorno alla normalità. Si può comunque usare, per esempio, il termine di *continuità in fase di emergenza*.

Continuità della sicurezza delle informazioni

La ISO/IEC 27001 usa l’espressione *Continuità della sicurezza delle informazioni* e la ISO/IEC 27000 la definisce come “processi per assicurare la continuità delle attività di sicurezza delle informazioni”.

Si tratta quindi di garantire che i processi di sicurezza (tra cui: monitoraggio, controllo degli accessi e prevenzione delle intrusioni fisiche e informatiche) siano mantenuti anche quando è attivato il BCP.

Il piano di disaster recovery potrebbe non considerare alcun intervento umano per il ripristino dei sistemi informatici, ma la continuità della sicurezza delle informazioni deve invece assicurare che siano presenti persone capaci di monitorare i sistemi e gestire alcuni processi fondamentali durante il periodo di emergenza.

La continuità della sicurezza delle informazioni deve anche considerare le informazioni in formato non digitale, quindi meno facili da duplicare e mantenere sicure nei siti secondari.

I parametri di continuità

I parametri di continuità si distinguono in *informatici* e *di processo*.

I parametri informatici sono:

- RTO (o *Recovery time objective)*, ossia il tempo previsto di ripristino (in emergenza) dei sistemi informatici;
- RPO (o *Recovery point objective*), ossia i dati che si prevede di perdere con il ripristino.

L’RPO corrisponde, indicativamente, all’ultimo backup o all’ultima sincronizzazione dei server tra quelli nel sito primario e quelli del sito di *disaster recovery*, se previsti.

Non è condiviso il nome di un parametro fondamentale: le prestazioni (e quindi le risorse) minime da garantire quando è attivato il sito di *disaster recovery*.

I parametri di processo sono:

- MTPD (o *Maximum tolerable period of disruption*), ossia il tempo massimo che un processo può non essere disponibile; il parametro RTO deve essere sempre minore del parametro MTPD; in altre parole, i sistemi informatici significativi devono essere ripristinati prima dei processi che li usano;
- MBCO (o *Minimum Business Continuity Objective*), ossia le prestazioni (e quindi le risorse, come per esempio persone, scrivanie e macchine) minime che un processo deve garantire.

Per quanto riguarda le informazioni non digitali, non è stato definito un termine corrispondente al RPO, ma va comunque considerato il tempo che intercorre tra la creazione o acquisizione di un documento e la messa in sicurezza di un suo duplicato in un sito secondario.

RTO e MTPD servono per stabilire il tempo massimo per ripristinare sistemi informatici e processi nella fase di emergenza. Non è previsto un termine per indicare il massimo tempo per cui può durare la fase di emergenza.

Considerando che le fasi di emergenza, fino al ritorno alla normalità, possono essere numerose (per esempio si può distinguere tra fase di emergenza immediata e emergenza non immediata), lo standard ISO 22301 usa il termine cumulativo di *prioritized timeframes* (tradotto in italiano come “priorità in termini di tempo”).

A cura di: **Cesare Gallotti**