

RPO e RT0: come progettare il disaster recovery



In questo articolo parleremo ancora di **business continuity**, ovvero di *business continuity plan* ed in particolare della progettazione delle procedure di **disaster recovery**.

Molte organizzazioni che non predispongono un vero e proprio piano di continuità operativa (o *business continuity plan*, BCP), comunque hanno una **procedura di disaster recovery**, più o meno evoluta. Purtroppo, però, questa attività viene delegata quasi interamente ai responsabili ICT senza coinvolgere il management, i responsabili dei processi primari di business ed in particolare di quelli più critici.

Non che i responsabili ICT non siano in grado di progettare una procedura di *disaster recovery* adeguata, ma spesso sono loro stessi che stabiliscono i requisiti di base del *disaster recovery*, ovvero implicitamente definiscono gli obiettivi **RT0** e **RPO** che dovrebbero essere alla base della procedura.

Riprendiamo le definizioni di questi indici, già esposte in precedenti articoli, per capire meglio di cosa si tratta.

- **Recovery Point Objective (RPO)** ovvero il punto (l'istante nel tempo) al quale le informazioni sono coerenti e possono essere ripristinate per consentire la ripresa delle attività (denominato anche *Maximum Data Loss*).
- **Recovery Time Objective (RT0)**: periodo di tempo entro il quale i servizi erogati, la produzione, i servizi di supporto e le funzionalità operative devono essere ripristinati dopo l'incidente che ha generato la discontinuità.

Facciamo un esempio per comprendere meglio il significato degli indici sopra esposti.

Supponiamo che una piccola organizzazione che opera nel settore dei servizi, denominata ALFA srl, decida di effettuare un **backup incrementale** dei propri dati con frequenza giornaliera su un NAS interno, mantenendo le ultime 7 versioni dei dati e che poi, per cautelarsi a fronte di eventuali catastrofi naturali che potrebbero

rendere inutilizzabile il sistema informatico aziendale e tutti i backup salvati su NAS, effettui anche un **backup completo** su nastri DAT con cadenza settimanale. I nastri magnetici dell'ultimo backup settimanale sono conservati a casa del titolare, a 20 km di distanza dalla sede dell'azienda, il quale quando si porta via il backup restituisce quello della settimana precedente.

Qual è il valore di RPO e RT0 per questa azienda?

Occorre distinguere fra diversi tipi di problemi (disastro):

1. Si tratta di un crash del sistema che ha comportato la perdita dei soli dati (eventualmente anche dei supporti di memorizzazione) oppure
2. Si tratta di un evento catastrofico che ha reso inutilizzabile l'intero server e l'infrastruttura informatica della sede di ALFA?

Evidentemente nel primo caso potrebbero essere sufficienti i backup su supporto NAS da ripristinare su un nuovo hard disk, reperibile in tempi brevi. Dunque il RT0 potrebbe essere pari anche ad una sola giornata, dipende dal tempo che si impiega a ripristinare il sistema (tempi di acquisto dei nuovi supporti di memorizzazione, tempi di eventuale reinstallazione del sistema operativo del server e degli applicativi, ecc.). Il RPO invece è pari ad una giornata di lavoro o meno, a seconda dal tempo trascorso dall'ultimo backup giornaliero eseguito. In questo caso per valutare correttamente il RT0 occorre capire quanto tempo si impiegherebbe a reinstallare il sistema, partendo dai supporti originali oppure da un'immagine del sistema creata attraverso l'impiego di macchine virtuali. Questa seconda soluzione, certamente più costosa della prima, potrebbe abbassare drasticamente il RPO.

Nel secondo caso il ripristino dell'operatività dipende anche dai danni generati alla sede dell'organizzazione: che si sia verificato un terremoto che ha reso inagibili i locali oppure un'alluvione i cui danni possano essere riparati entro qualche giorno o settimane la situazione può essere sensibilmente differente e il RT0, anche in questo caso può essere di alcuni giorni o settimane, indipendentemente dalla strategia di backup implementata. Il backup settimanale su nastro, conservato in un luogo sicuro (da valutare se la distanza dalla sede è sufficiente per garantire un'alta probabilità di evitare danni), garantirebbe un RPO di al massimo una settimana di dati persi.

Bisogna capire se questi valori, di RPO e RT0, sono accettabili per l'organizzazione oppure le perdite, in termini di dati e di discontinuità operativa, mettono a repentaglio la sopravvivenza dell'azienda.

Ricordiamo che per alcune attività critiche il verificarsi di eventi disastrosi con RT0 di settimane e di RPO di una settimana potrebbero portare a danni economici ingenti, non coperti da polizze assicurative (ritardi nella consegna di commesse con addebito di penali da parte del committente, perdita di commesse importanti, ecc.).

In questa seconda situazione occorrerebbe certamente un **sito di *disaster recovery***, ovvero un sito alternativo, geograficamente distante dalla sede principale dell'azienda, in grado di consentire la ripresa dell'attività in pochissimo tempo (ore, al massimo una giornata lavorativa) e la perdita dei dati di al massimo una giornata, dunque ottenendo un RTO = 1 giorno e RPO = 1 giorno. Ciò potrebbe essere ottenuto senza investimenti consistenti in una struttura gemella, ma dotandosi di una infrastruttura tecnologica in *cloud*.

In conclusione la procedura di *disaster recovery* dovrebbe essere progettata da personale competente (responsabile IT, consulenti esterni, ...) basandosi su precisi input da parte della Direzione aziendale, derivanti da obiettivi di RPO e RTO ritenuti adeguati per l'organizzazione. La procedura di *disaster recovery* progettata avrà dei costi (che possono variare in base alle soluzioni scelte) che la Direzione dovrà mettere a budget per garantirsi gli obiettivi desiderati. Viceversa bisognerà migrare verso obiettivi meno ambiziosi di RPO e RTO, ma la Direzione deve essere consapevole di ciò. In caso di disastri, infatti, nessuno potrà accusare altri di non aver pensato alle giuste contromisure ed ognuno si assumerà le responsabilità che gli spettano.

La sicurezza delle informazioni in caso di calamità naturali e non naturali



In caso di catastrofi e calamità naturali quali terremoti, alluvioni, inondazioni, incendi, eruzioni vulcaniche, uragani oppure atti terroristici, uno dei danni collaterali dopo la perdita di vite umane e i danni materiali ad edifici ed infrastrutture, occorre considerare il blocco dei sistemi informativi che può rallentare notevolmente la ripresa delle normali attività.

Le metodologie da impiegare per prevenire e mitigare i danni che possono compromettere la ripresa delle attività dopo un evento catastrofico riguardano la tematica della business continuity (continuità operativa).

Nell'intervento presentato lo scorso 17/11 al [Convegno EVENTI SISMICI: PREVENZIONE, PROTEZIONE, SICUREZZA, EMERGENZA](#), le cui slide sono scaricabili in questa pagina, si sono presentate tutte le attività da porre in essere per controllare tali

situazioni indesiderate, in particolare sono stati trattati i seguenti argomenti:

- business continuitymanagement
- normative ISO 22301, ISO 2001/27002 e ISO 27031 per la gestione della business continuity, con particolare riferimento ai sistemi informatici
- gestione dei rischi per la continuità operativa
- disaster recovery
- obiettivi ed indicatori di business continuity
- business continuity plan (piano di continuità operativa).





[La sicurezza dei dati in caso di terremoto \(240 download\)](#)

La nuova edizione della norma ISO 27002 (seconda parte)



In questo articolo (cfr. [precedente articolo](#)) passiamo ad esaminare la seconda parte della norma La norma UNI CEI ISO/IEC 27002:2014 – *Raccolta di prassi sui controlli per la sicurezza delle informazioni* (che sostituisce la ISO 27002:2005).

12 Sicurezza delle attività operative

Questa area comprende ben 7 categorie:

- **Procedure operative e responsabilità (12.1):** devono essere predisposte procedure

per documentare lo svolgimento di una serie di attività inerenti la sicurezza, occorre gestire i cambiamenti all'organizzazione e la capacità delle risorse (di *storage*, di banda, infrastrutturali ed anche umane), infine è necessario mantenere separati gli ambienti di sviluppo da quelli di produzione.

- **Protezione dal malware (12.2):** un solo controllo in questa categoria (protezione dal malware) che prescrive tutte le misure di sicurezza da attuare contro il malware. Non solo antivirus per prevenire ed eliminare malware, ma anche azioni di prevenzione tecnica e comportamentali (consapevolezza degli utenti).
- **Backup (12.3):** devono essere documentate ed attuate procedure di backup adeguate a garantire il ripristino dei dati in caso di perdita dell'integrità degli stessi e la continuità operativa (vedasi anche punto 17).
- **Raccolta di log e monitoraggio (12.4):** devono essere registrati, conservati e protetti i log delle attività degli utenti normali e di quelli privilegiati (si ricorda che per apposita disposizione del Garante Privacy italiano i log degli accessi in qualità di Amministratore di Sistema devono essere mantenuti in modo "indelebile" per almeno 6 mesi), occorre inoltre mantenere sincronizzati gli orologi dei sistemi con una fonte attendibile.
- **Controllo del software di produzione (12.5):** particolari attenzioni devono essere adottate nell'installazione ed aggiornamento del software di produzione (non solo per organizzazioni del settore ICT, banche o assicurazioni, ma anche per aziende manifatturiere!).
- **Gestione delle vulnerabilità tecniche (12.6):** viene fornita dalla norma un'ampia guida attuativa sulla gestione delle vulnerabilità tecniche conosciute (occorre mantenere un censimento dell'hardware e del relativo software installato su ogni elaboratore, installare le *patch* di sicurezza in modo tempestivo, mantenersi aggiornati sulle vulnerabilità di sicurezza conosciute, ecc.), oltre alle indicazioni sulla limitazione nell'installazione dei software (è opportuno, infatti, ridurre al minimo la possibilità per gli utenti di installare applicativi software autonomamente, anche se leciti come le utility gratuite che, a volte, possono essere il veicolo di *adware* o altre minacce alla sicurezza).
- **Considerazioni sull'audit dei sistemi informativi (12.7):** gli audit sui sistemi informativi dovrebbero avere un impatto ridotto sulle attività lavorative e le evidenze raccolte dovrebbero essere raccolte senza alterare i dati dei sistemi (accessi in sola lettura) e dovrebbero essere mantenute protette.

Questi elementi nella precedente versione della norma erano in gran parte all'interno della sezione 10 "*Communications and Operations Management*" (ma la gestione delle vulnerabilità tecniche era, invece, al paragrafo 12.6, per puro caso lo stesso della versione attuale della norma), il quale comprendeva anche i controlli del punto 13 seguente.

13 Sicurezza delle comunicazioni

Questa sezione contiene due sole categorie:

- **Gestione della sicurezza della rete (13.1):** occorre adottare alcuni accorgimenti per garantire la sicurezza delle reti interne (responsabilità, autenticazioni, ecc.); viene anche citata la ISO/IEC 27033 nelle sue parti da 1 a 5 sulla sicurezza delle reti e delle comunicazioni per ulteriori informazioni. Deve, inoltre, essere gestita la sicurezza dei servizi di rete, compresi i servizi acquistati presso fornitori esterni, e la segregazione delle reti (separazione delle VLAN, gestione delle connessioni Wi-Fi, ...).
- **Trasferimento delle informazioni (13.2):** occorre stabilire ed attuare politiche e procedure per il trasferimento delle informazioni con qualsiasi mezzo (posta elettronica, fax, telefono, scaricamento da internet, ecc.), nel trasferimento di informazioni con soggetti esterni occorre stabilire accordi sulle modalità di trasmissione, le informazioni trasmesse tramite messaggistica elettronica dovrebbero essere adeguatamente controllate e protette (non solo e-mail, ma anche sistemi EDI, *instant messages*, *social network*, ecc.) e, infine, occorre stabilire e riesaminare periodicamente accordi di riservatezza e di non divulgazione con le parti interessate.

I 7 controlli di quest'area sono sicuramente molto dettagliati e migliorano, oltre ad aggiornare, la precedente versione della norma, includendo controlli (un po' sparsi nella versione 2005 della ISO 27002) che recepiscono le nuove modalità di comunicazione, tra cui i social network, professionali e non.

14 Acquisizione, sviluppo e manutenzione dei sistemi

Quest'area tratta la sicurezza dei sistemi informativi impiegati per le attività aziendali e comprende tre categorie:

- **Requisiti di sicurezza dei sistemi informativi (14.1):** la sicurezza dei sistemi informativi- acquistati o sviluppati ad hoc – deve essere stabilita fin dall'analisi dei requisiti, deve essere garantita la sicurezza dei servizi applicativi che viaggiano su reti pubbliche (ad esempio attraverso trasmissioni ed autenticazioni sicure crittografate), infine occorre garantire la sicurezza delle transazioni dei servizi applicativi.
- **Sicurezza nei processi di sviluppo e supporto (14.2):** devono essere definite ed attuate politiche per lo sviluppo (interno o esterno all'organizzazione) sicuro dei programmi applicativi, devono essere tenuti sotto controllo tutti i cambiamenti ai sistemi (dagli aggiornamenti dei sistemi operativi alle modifiche dei sistemi gestionali), occorre effettuare un riesame tecnico sul funzionamento degli applicativi critici a fronte di cambiamenti delle piattaforme operative (sistemi di produzione, database, ecc.) e si dovrebbero limitare le modifiche (personalizzazioni) ai pacchetti software, cercando comunque di garantirne i futuri aggiornamenti. Inoltre dovrebbero essere stabiliti, documentati ed attuati principi per l'ingegnerizzazione sicura dei sistemi informatici e per l'impiego di ambienti di sviluppo sicuri. Nel caso in cui attività di sviluppo software fossero commissionate all'esterno, dovrebbero essere stabilite misure per il controllo del processo di sviluppo externalizzato. Infine dovrebbero

essere eseguiti test di sicurezza dei sistemi durante lo sviluppo e test di accettazione nell'ambiente operativo di utilizzo, prima di rilasciare il software.

- **Dati di test (14.3):** i dati utilizzati per il test dovrebbero essere scelti evitando di introdurre dati personali ed adottando adeguate misure di protezione, anche al fine di garantirne la riservatezza.

Nel complesso i 13 controlli di questa sezione sono molto dettagliati e comprendono una serie di misure di sicurezza informatica ormai consolidate che riguardano tutti gli aspetti del ciclo di vita del software impiegato da un'organizzazione per la propria attività. Alcuni principi vanno commisurati ad una attenta valutazione dei rischi, poiché una stessa regola di sicurezza informatica (ad es. l'aggiornamento sistematico e tempestivo del software di base) potrebbe non garantire sempre l'integrità e la disponibilità dei sistemi (ad es. errori o malfunzionamenti introdotti dagli ultimi aggiornamenti di un sistema operativo).

15 Relazioni con i fornitori

Questo punto di controllo tratta tutti gli aspetti di sicurezza delle informazioni che possono legati al comportamento dei fornitori. Sono state individuate due categorie:

- **Sicurezza delle informazioni nelle relazioni con i fornitori (15.1):** è necessario stabilire una politica ed accordi su tematiche inerenti la sicurezza delle informazioni con i fornitori che accedono agli asset dell'organizzazione; tali accordi devono comprendere requisiti per affrontare i rischi relativi alla sicurezza associati a prodotti e servizi nella filiera di fornitura dell'ICT (cloud computing compreso).
- **Gestione dell'erogazione dei servizi dei fornitori (15.2):** occorre monitorare – anche attraverso audit se necessario – e riesaminare periodicamente le attività dei fornitori che influenzano la sicurezza delle informazioni, nonché tenere sotto controllo tutti i cambiamenti legati alle forniture di servizi.

16 Gestione degli incidenti relativi alla sicurezza delle informazioni

L'area relativa agli incidenti sulla sicurezza delle informazioni (sezione 13 della precedente versione della norma) comprende una sola categoria (erano 2 nella precedente edizione):

- **Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti (16.1):** devono essere rilevati e gestiti tutti gli incidenti relativi alla sicurezza delle informazioni (viene qui richiamata la [ISO/IEC 27035](#) – *Information security incident management*), ma anche rilevate ed esaminate tutte le segnalazioni di eventi relativi alla sicurezza che potrebbero indurre a pensare che qualche controllo è risultato inefficace senza provocare un vero e proprio incidente e pure tutte le possibili debolezze dei controlli messi in atto. In ogni caso ogni evento relativo alla sicurezza delle

informazioni va attentamente valutato per eventualmente classificarlo come incidente vero e proprio o meno. Occorre poi rispondere ad ogni incidente relativo alla sicurezza delle informazioni in modo adeguato ed apprendere da quanto accaduto per evitare che l'incidente si ripeta. Infine dovrebbero essere stabilite procedure per la raccolta di evidenze relative agli incidenti e la successiva gestione (considerando anche eventuali azioni di analisi forense).

17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

In quest'area (corrispondente al punto 14 della precedente versione della norma) viene trattata la **business continuity** in 5 controlli suddivisi in due categorie:

- **Continuità della sicurezza delle informazioni (17.1):** la continuità operativa per la sicurezza delle informazioni dovrebbe essere pianificata a partire dai requisiti per la business continuity, piani di continuità operativa (*business continuity plan*) dovrebbero essere attuati, verificati e riesaminati periodicamente.
- **Ridondanze (17.2):** per garantire la disponibilità (e la continuità operativa) occorre prevedere architetture e infrastrutture con adeguata ridondanza.

Naturalmente sull'argomento esiste la norma specifica UNI EN ISO 22301:2014 – *Sicurezza della società – Sistemi di gestione della continuità operativa – Requisiti*.

18 Conformità

Questo ultimo punto di controllo (era il punto 15 nella ISO 27002:2005) tratta la gestione della cosiddetta "*compliance*", ovvero la conformità a leggi, regolamenti ed accordi contrattuali con i clienti. Sono identificate due categorie:

- **Conformità ai requisiti cogenti e contrattuali (18.1):** occorre innanzitutto identificare i requisiti cogenti, quindi attuare controlli per evitare di ledere i diritti di proprietà intellettuale, proteggere adeguatamente le registrazioni che permettono di dimostrare la conformità a tutti i requisiti cogenti, in particolare devono essere rispettati leggi e regolamenti sulla privacy (in Italia il D.Lgs 196/2003 in attesa del nuovo Regolamento Europeo, ma nella norma viene citata come riferimento la ISO/IEC 29100:2011 "*Information technology – Security techniques – Privacy framework*"). Infine occorre considerare eventuali limitazioni all'uso dei controlli crittografici vigenti in alcune nazioni.
- **Riesami della sicurezza delle informazioni (18.2):** dovrebbe essere svolto periodicamente un riesame indipendente sulla sicurezza delle informazioni dell'organizzazione, i processi di elaborazione delle informazioni e le procedure dovrebbero essere riesaminate periodicamente per valutarne la continua conformità ed adeguatezza alla politica ed alle norme ed infine dovrebbero essere eseguite delle verifiche tecniche della conformità dei sistemi informativi a politiche e standard di sicurezza (ad esempio *penetration test* e

vulnerability assessment). Su quest'ultimo controllo si fa riferimento alla ISO/IEC TR 27008 – *Guidelines for auditors on information security management systems controls*.

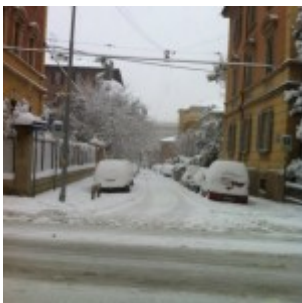
Business Continuity Plan, questo sconosciuto



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 neviccate 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)

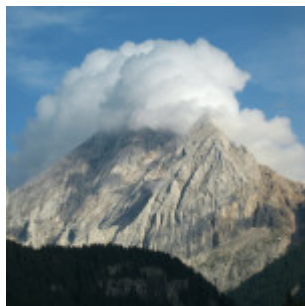
2. Manutenzione del BCP

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.

[\[Download non trovato\]](#)

Cosa hanno in comune privacy, cloud computing e business continuity?



In precedenti articoli ([Il cloud computing e la PMI](#), [i sistemi di gestione della sicurezza delle informazioni](#), [ISO 22301 e la business continuity](#), [le novità sulla privacy](#)) abbiamo affrontato tutti questi argomenti che, indubbiamente, hanno un unico filo conduttore.

Oggi molte aziende, fra cui anche numerose PMI, hanno dati “nel *cloud*”, ovvero memorizzati in risorse fisiche non collocate all’interno dell’azienda, bensì su internet, magari senza rendersene conto. Infatti, oltre a veri e propri servizi *cloud* erogati da fornitori specializzati, molte PMI utilizzano servizi di archiviazione gratuiti quali SkyDrive, Dropbox o Google Drive in maniera non strutturata, in quanto sono propri reparti o uffici o addirittura singoli collaboratori che, per praticità, hanno pensato di sfruttare suddetti *tool* di archiviazione remota.

In altri casi alcune organizzazioni utilizzano software via web che memorizzano i dati su server remoti, magari presso il fornitore del software (spesso si tratta di *Saas, Software as a Service*).

Tra i principali aspetti negativi che hanno generato diffidenza sull’archiviazione nel *cloud* c’è sicuramente la **sicurezza dei dati**, declinata in termini di **riservatezza**. Molti imprenditori, infatti, hanno la sensazione che alcuni dati riservati (informazioni commerciali, proprietà intellettuale relativa a progetti, ecc.) debbano rimanere in azienda per paura che qualcuno li possa consultare.



Normalmente una PMI, specialmente una piccola impresa, non effettua un’adeguata **valutazione dei rischi** che corre e, pertanto, valuta questo argomento a sensazione, piuttosto che con fatti concreti. Quali sono infatti i rischi reali?

In una logica di *Risk Assessment*, naturalmente, ogni impresa fa storia a se; bisogna conoscere quali dati vorrebbe mettere sul cloud, qual è il livello di riservatezza che tali dati devono avere, se si tratta di dati sensibili, quali **procedure di backup** sono implementate, di che tipo di **connessione internet** si dispone e così via.

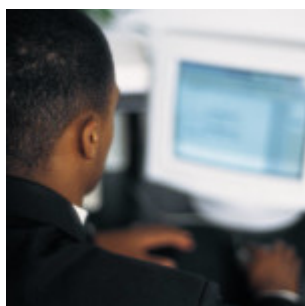
In linea generale parlare di dati poco sicuri nel *cloud* perché si teme che qualcuno possa “guardarci dentro” non ha molto senso: a parte che bisognerebbe valutare quale livello di sicurezza ci si aspetta per ogni tipo di dato (si veda il precedente articolo sulla [valutazione dei rischi per la sicurezza delle informazioni](#)), oggi

molti *repository* di dati nel *cloud* forniscono ampie garanzie di sicurezza, soprattutto se sono gestiti da importanti player del settore, quali Microsoft, Google, Amazon, ecc.

Se, come al solito, decliniamo il termine **Sicurezza** in **Riservatezza, Integrità e Disponibilità** (ISO 27000 *docet*) e valutiamo nel complesso **il livello di rischio che incombe sui dati nel cloud**, vediamo che, a fronte di un **livello di riservatezza più che adeguato** (i dati di una PMI nel cloud normalmente sono sufficientemente protetti da sguardi indiscreti, grazie alle misure di sicurezza informatica che i fornitori più seri offrono ormai per *default*), certamente superiore a quello che si può ottenere all'interno dell'azienda stessa (dove potrebbero esserci soggetti interessati a curiosare dove non dovrebbero) la garanzia di **integrità dei dati** è più che buona, ma sulla **disponibilità** degli stessi occorre fare qualche riflessione.

Su quest'ultimo aspetto incide non solo l'affidabilità del fornitore di servizi *cloud* e dell'infrastruttura di cui dispone, ma anche la **connessione internet** che, ancora oggi, non è sicuramente adeguata in molte imprese italiane, sia per **velocità**, sia per **continuità del servizio**. È proprio questo l'anello di congiunzione con la **continuità operativa**, più elegantemente detta **business continuity**.

Infine la **privacy**, ovvero la **protezione dei dati personali** con la relativa legge italiana (D.Lgs 196/2003) ed il **nuovo Regolamento Europeo** che sarà emanato probabilmente il prossimo anno. In questo ambito un Parere della Commissione Europea del 2012 ha per il momento fugato molti dubbi sulle garanzie legali che un'impresa dovrebbe richiedere al proprio fornitore di servizi cloud per essere tranquilla di non incorrere in pesanti problemi legali.



Probabilmente molti **contratti** che regolamentano la fornitura di servizi *cloud* (spesso mascherati sotto la fornitura di *software as a service*) non cautelano adeguatamente l'organizzazione che, non dimentichiamolo, è **titolare del trattamento dei dati** memorizzati in un server chissà dove. È prassi consolidata, infatti, di numerosi fornitori di SaaS di spostare i database dei propri clienti nello spazio web più conveniente per rapporto qualità/prezzo, non importa se in Canada o in

Australia In tali situazioni le aziende non dovrebbero dimenticare che come titolari del trattamento sono i **responsabili di fronte alla legge su eventuali inosservanze del Codice della Privacy** e che "esportare" i dati personali fuori dalla Comunità Europea non è sempre possibile, come minimo occorre richiedere il consenso dell'interessato.

Dunque quali interrogativi deve porsi un'azienda coscienziosa prima di affidare i propri dati al *cloud*?

Vediamo i principali, fermo restando che solo dopo una precisa valutazione dei rischi si può determinare quali aspetti sono più critici in ogni singola realtà.

1. Il contratto con il fornitore mi garantisce adeguatamente rispetto alla normativa sulla privacy?
2. Il livello di riservatezza necessario sui dati è adeguatamente garantito da misure di sicurezza dichiarate contrattualmente dal fornitore?
3. La disponibilità dei dati garantita contrattualmente (SLA) è adeguata alle mie esigenze?
4. Posso rientrare in possesso dei miei dati quando voglio e senza costi eccessivi?
5. Il fornitore è sufficientemente affidabile? Si serve di subfornitori egualmente affidabili e resi noti contrattualmente?
6. In caso di perdita dei dati quali sistemi di *disaster recovery* mi garantiscono di rientrare operativo nel più breve tempo possibile? Tale tempo è coerente con le mie esigenze operative?
7. So esattamente in quale stato o area geografica sono memorizzati i miei dati?
8. Ho considerato tutti i possibili fattori di rischio che possono incombere sulla mia continuità operativa?
9. Ho definito gli obiettivi di disponibilità del servizio e di *business continuity* in caso di situazione di crisi?
10. Sono in grado di monitorare il comportamento del fornitore ed eventualmente sottoporlo ad audit sul rispetto dei vincoli contrattuali?

Oggi esistono molti sistemi per garantirsi un futuro tranquillo con i dati nel *cloud*, ad esempio seguendo i principi ed i metodi indicati dalle **norme della famiglia ISO 27000** (ISO 27001 che riporta i requisiti di un **sistema di gestione della sicurezza delle informazioni** certificabile, ISO 27002 che riporta le *best practices*, ovvero i controlli che possono essere messi in atto, ISO 27005 che è la linea guida per il *risk assessment*, ...) includendovi i requisiti cogenti per la privacy in vigore in Italia ed in Europa. Se il problema di mantenere una certa continuità operativa costituisce un fattore critico si può adottare la metodologia esposta nella ISO 22301 ed in altri standard e linee guida sull'argomento.

Mediante gli stessi sistemi ci si può garantire in modo adeguato nei confronti del fornitore, ad esempio esaminando il contratto con un supporto legale competente, verificare se il fornitore dispone di certificazioni ISO 9001, ISO 27001, ISO 22301 oppure dispone di un Report SSAE 16 ("*Statement on Standards for Attestation Engagements*" n. 16 , standard AICPA per il reporting sui controlli alle organizzazioni che forniscono servizi in outsourcing, richiesto dalle aziende soggette al *Sarbanes-Oxley Act* o SOX, Sezione 404).

Se ascoltiamo quello che ci raccontano gli esperti di sicurezza informatica che relazionano nei frequenti seminari o convegni sull'argomento non c'è certo da stare tranquilli nemmeno all'interno della propria azienda (tra *ransomware* e *data leakage* ogni tanto nascono minacce sempre più terrificanti per il futuro delle nostre imprese, senza dimenticare il comportamento dei collaboratori disonesti) e, quindi, un cloud consapevole può veramente essere una buona cosa.

Dall'altra parte la *software house* che fornisce applicazioni *web-based* con l'opzione

di memorizzare i dati, anziché su un server interno all'azienda, su un server remoto (ovvero nel *cloud*) dovrebbe prendere in considerazione tutti gli aspetti sopra esposti, sia al fine di fornire un servizio pienamente conforme alle normative applicabili e di piena soddisfazione di tutte le esigenze del cliente, sia al fine di non incorrere in problemi legali nel caso in cui qualcosa andasse storto, anche solo a causa del proprio fornitore di servizi cloud. Dunque valutare quali tipi di dati verranno archiviati nel cloud dai propri clienti e quali garanzie forniscono i fornitori di spazio di archiviazione a cui ci si rivolge (le **caratteristiche di un data center sicuro** sono state esposte in un [articolo apparso lo scorso anno sulla rivista INARCOS](#)).

In conclusione, come per qualsiasi decisione o progetto strategico, le aziende (clienti e fornitori) dovrebbero valutare con adeguate competenze la situazione nel suo complesso ed i rischi che si potrebbe correre. Purtroppo tali competenze, informatiche, legali e gestionali spesso non sono presenti in piccole realtà poco strutturate che, quindi, rischiano di incorrere in problemi significativi e se poi trattano dati sensibili, in particolare dati sanitari, potrebbero veramente incorrere in perdite economiche e di immagine molto importanti.

La norma ISO 22301 per la certificazione della business continuity



Lo standard ISO 22301 (*Societal security – Business continuity management systems – Requirements*) specifica i requisiti per progettare, implementare e gestire efficacemente un **Sistema di gestione della continuità operativa**.

Il sistema di gestione della continuità operativa (*business continuity management system* o BCMS) enfatizza l'importanza di:

- comprendere le esigenze dell'organizzazione e le necessità per stabilire la politica e gli obiettivi di un sistema di gestione per la continuità del business;
- implementare e rendere operativi controlli e misure per gestire la capacità di

un'intera organizzazione nella gestione delle interruzioni dell'operatività dovute a cause accidentali;

- monitorare e riesaminare le prestazioni e l'efficacia del sistema di gestione della continuità operativa
- del miglioramento continuo del BCMS basato su obiettivi misurabili.

Si noti che anche la norma ISO/IEC 27031 "*Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*" tratta la business continuity, ma nel contesto dell'ICT e delle tecniche di sicurezza strettamente correlata alla **ISO 27001** che contiene i **requisiti per la certificazione dei sistemi di gestione della sicurezza delle informazioni**.

La ISO 22301 evidenzia i componenti chiave del sistema di gestione della continuità operativa, peraltro presenti anche in altri sistemi di gestione. Tra essi la **politica**, le **persone** con le loro **responsabilità** definite, la **gestione dei processi** correlati a politica, pianificazione, attuazione ed operatività del BCMS, **valutazione delle prestazioni**, **riesame della direzione** e **miglioramento**, nonché la **documentazione** in grado di fornire evidenze verificabili tramite **audit** sul sistema di gestione della continuità operativa.

Anche questa norma introduce il metodo del "**PLAN DO CHECK ACT**" già noto da altre norme dei sistemi di gestione. In particolare il modello PDCA del sistema di gestione della continuità operativa ha come input le **parti interessate** (clienti, proprietà/soci, dipendenti/collaboratori, fornitori, collettività) e i **requisiti per la business continuity**, mentre l'output del sistema è fornito alle stesse parti interessate ed è costituito dalla **continuità operativa gestita**.

Per questa norma il concetto di "parti interessate" o *stakeholders* è importante in quanto una discontinuità nell'operatività dell'organizzazione, una indisponibilità dei servizi essenziali per i clienti, un fermo delle attività produttive per un periodo più o meno lungo, possono causare danni non solo all'organizzazione stessa, ma soprattutto ai clienti che usufruiscono dei suoi prodotti/servizi e che quindi non riescono a lavorare proficuamente, ai fornitori che non possono rifornire i loro prodotti/servizi, ecc..

Scopo della norma per la gestione della *business continuity* è quello di specificare i requisiti atti a pianificare, stabilire, implementare, realizzare, monitorare, riesaminare, mantenere e migliorare in modo continuo un sistema di gestione documentato per proteggersi contro gli incidenti che possono accadere e fermare l'organizzazione, ma non solo. Il BCMS ha anche l'obiettivo di ridurre la probabilità che tali eventi negativi avvengano, prepararsi ad essi e rispondere in modo adeguato per ripristinare l'operatività nel più breve tempo possibile qualora l'incidente che causa lo stato di crisi si verifichi.

La norma ISO 22301 definisce alcuni termini specifici sulla materia, tra cui il

termine business continuity, **business continuity management system**, **business impact analysis** (BIA) ossia analisi di impatto sull'operatività dell'organizzazione.

Oltre ad altri termini consueti delle norme della serie ISO 9000 compare il nuovo termine **informazione documentata**, che ritroveremo nella nuova edizione della norma ISO 9001. Altro termine significativo mutuato dalle norme della serie ISO 27000 è quello di **incidente** che è definito come una situazione che potrebbe rappresentare o potrebbe portare a una distruzione, una perdita, uno stato di emergenza o una crisi. Al proposito la norma utilizza spesso il termine *disruption* che rappresenta un atto o un evento che interrompe la continuità (e genera discontinuità).

Sono anche fornite le classiche definizioni legate alla **gestione del rischio** (risk assessment, risk management, rischio) tra cui il *risk appetite* («*amount and type of risk that an organization is willing to pursue or retain*») ovvero la **propensione al rischio** dell'organizzazione che, si vedrà in seguito, dovrà essere identificata al fine di intraprendere azioni di prevenzione idonee.

Vengono poi definiti degli indicatori specifici per questa tematica come:

- **Maximum Acceptable Outage** (MAO) ovvero il tempo massimo ritenuto accettabile che può trascorrere – a fronte di un evento avverso – durante il quale non viene fornito un prodotto/servizio o non viene svolta un'attività.
- **Maximum Tolerable Period of Disruption** (MTPD) ovvero il tempo massimo tollerabile che può trascorrere a fronte degli impatti negativi conseguenti ad un incidente come risultato della mancata fornitura di un prodotto, erogazione di un servizio o svolgimento di un'attività operativa. Si noti che rispetto al MAO precedente il MTPD è un periodo potenzialmente superiore in quanto si può presumere che gli impatti negativi di una interruzione di un servizio possano durare più a lungo dell'interruzione stessa.
- **Minimum Business Continuity Objective** (MBCO) che rappresenta il livello di servizio minimo accettabile dall'organizzazione per raggiungere i propri obiettivi di business durante una l'interruzione della continuità dovuta all'incidente (periodo di crisi)
- **Recovery Point Objective** (RPO) ovvero il punto (l'istante nel tempo) al quale le informazioni sono coerenti e possono essere ripristinate per consentire la ripresa delle attività (denominato anche *Maximum Data Loss*).
- **Recovery Time Objective** (RTO): periodo di tempo entro il quale i servizi erogati, la produzione, i servizi di supporto e le funzionalità operative devono essere ripristinati dopo l'incidente che ha generato la discontinuità.

Il capitolo 4 della norma denominato "Contesto dell'organizzazione" – che ritroveremo nella nuova ISO 9001 del 2015 – contiene gli elementi per comprendere il contesto dell'organizzazione (punto 4.1 della norma). La norma stabilisce che nell'ambito del Sistema di gestione per la continuità operativa debbono essere identificati **i bisogni dell'organizzazione e delle sue parti interessate**, che dovranno essere tenuti in debito conto nella progettazione del sistema di gestione

dell'organizzazione, la quale dovrà anche identificare e documentare le attività svolte dall'organizzazione stessa, le sue funzioni, i servizi, i prodotti e tutto ciò che è necessario per identificare i potenziali impatti legati a incidenti distruttivi che possono generare discontinuità operativa.

Inoltre dovranno essere documentati i collegamenti tra la politica per la continuità operativa e gli obiettivi dell'organizzazione e la sua politica, inclusa una strategia generale di gestione dei rischi e l'approccio dell'organizzazione ai rischi correlati alla *business continuity*, ovvero la propria propensione al rischio.

Al punto 4.2 sono descritti gli aspetti riguardanti la **comprensione delle esigenze delle parti interessate**, ovvero i requisiti legali e regolamentari cui l'organizzazione è soggetta. Ciò aiuterà nella **definizione dello scopo e campo di applicazione del sistema di gestione di continuità operativa** (4.3). A tale riguardo la norma stabilisce le modalità attraverso le quali l'organizzazione deve stabilire quali processi prodotti e servizi sono compresi nel sistema di gestione e quali parti dell'organizzazione agiscono all'interno di esso, dettagliando eventuali esclusioni che, comunque, non possono influenzare negativamente i risultati del sistema di gestione.

Al punto 4.4 la norma stabilisce che l'organizzazione deve implementare, mantenere attivo e migliorare continuamente un sistema di gestione della continuità operativa, inclusi i processi necessari e le relative interazioni fra essi, in accordo con i requisiti di questo standard internazionale (ISO 22301).

Il capitolo 5 della norma è denominato "**Leadership**". In esso la norma stabilisce che l'alta direzione (ovvero il *top management*) deve possedere leadership e dimostrare un impegno preciso rispetto al sistema di gestione per la continuità operativa. L'impegno del management viene poi esplicitato attraverso una serie di responsabilità della direzione relative al sistema di gestione quali, ad esempio, assicurare che politiche ed obiettivi siano stabiliti, che le risorse necessarie siano messe a disposizione e che vi sia un'adeguata comunicazione all'interno dell'organizzazione relativamente ai requisiti del sistema di gestione della continuità operativa.

Sono poi stabiliti requisiti relativi alla definizione della **politica per la continuità operativa** e la definizione della **struttura organizzativa dell'organizzazione**, quindi la definizione di ruoli responsabilità ed autorità. Questi ultimi due paragrafi risultano perfettamente simili a quelli delle altre norme sui sistemi di gestione, in particolare la nuova ISO 9001:2015.

Il capitolo 6 denominato "**Pianificazione**" stabilisce che:

- L'organizzazione deve porre in essere **azioni rivolte ai rischi ed alle opportunità**, in particolare assicurando che il sistema riesca a perseguire gli obiettivi ed i risultati stabiliti, prevenire o ridurre gli effetti indesiderati

e mirare al miglioramento continuo.

- Vengano definiti **obiettivi per la *business continuity*** e piani per raggiungerli; tale aspetto, con le dovute modifiche, è del tutto analogo ad altri sistemi di gestione: gli obiettivi devono essere misurabili, devono essere monitorati, occorre stabilire chi è responsabile, che cosa deve fare, quali risorse sono richieste, quando dovranno essere completate le azioni finalizzate al perseguimento degli obiettivi e come dovranno essere valutati i risultati. Unica differenza rispetto ad altri sistemi di gestione è che nella definizione degli obiettivi bisognerà tenere conto di un livello minimo di servizio o di prodotto fornito ritenuto accettabile dall'organizzazione nel raggiungimento dei suoi obiettivi.

Il capitolo 7 della norma denominato "**Supporto**" stabilisce i requisiti per alcune attività e processi di supporto, quali – in generale – la **gestione delle risorse**, le **competenze del personale**, la **consapevolezza** dello stesso personale relativamente al sistema di gestione della continuità operativa e la **comunicazione**, sia essa interna che esterna. In particolare, per questo tipo di sistema di gestione, le modalità ed i mezzi di comunicazione sono molto importanti per garantire la continuità del servizio anche durante i periodi di indisponibilità delle risorse critiche.

Infine l'ultimo paragrafo di questo capitolo è dedicato alle **informazioni documentate**, in completa analogia con il nuovo schema delle norme relative ai sistemi di gestione. I requisiti relativi alle informazioni documentate riguardano le modalità di gestione di documenti, dei dati e delle registrazioni richieste dalla norma.

A questo riguardo è opportuno precisare che, nell'ambito della *business continuity*, i documenti – in particolare le procedure e le istruzioni operative – necessarie per ripristinare nel più breve tempo possibile i servizi richiesti durante i periodi di crisi, dovrebbero essere accessibili dai responsabili nominati, dunque occorre prevedere supporti alternativi per i documenti che potrebbero non essere disponibili nel formato originario, su supporto elettronico o cartaceo. Pertanto tali documenti dovrebbero essere resi disponibili su supporti realmente utilizzabili in funzione del tipo di crisi (scenario) previsto in fase di pianificazione.

Il capitolo 8 della norma denominato "**Operation**", la cui traduzione in lingua italiana è piuttosto incerta, rappresenta il cuore di questa normativa ISO 22301 in quanto tratta gli aspetti di pianificazione e controllo dei processi operativi, la valutazione dei rischi e l'analisi di impatto, ovvero la **business impact analysis** (BIA), ed infine la **strategia di business continuity** ovvero tutto ciò che l'organizzazione intende fare per garantire la continuità operativa, compresa la definizione dei **business continuity plan** o **piani di continuità operativa**, la loro applicazione e test.

Nei suddetti paragrafi della sezione 8 vengono specificate, tra l'altro, le modalità di effettuazione e documentazione della *business impact analysis* (analisi gestionale

attraverso la quale un'organizzazione valuta quantitativamente e qualitativamente gli impatti e le perdite che possono risultare se l'organizzazione stessa subisce un grave incidente, nonché il livello minimo di risorse necessarie per il ripristino dell'operatività) e della **valutazione dei rischi**, per la quale può essere preso come riferimento quanto indicato nella **ISO 31000** (ora anche **UNI ISO 31000 – Gestione del rischio – Principi e linee guida**). Occorre precisare che sia l'analisi di impatto sia la valutazione dei rischi dovranno prendere in considerazione i rischi che possono impattare la continuità operativa, quindi i rischi che si verificano incidenti distruttivi che portino a situazioni di crisi o comunque di interruzione dell'operatività e, conseguentemente, a situazioni insostenibili per la propensione al rischio definita per l'organizzazione. A fronte di tali situazioni, in base ai risultati della valutazione dei rischi, dovranno essere determinate e poste in essere le azioni conseguenti per mantenere la continuità operativa.

Il capitolo 9 della norma tratta la "**Valutazione delle prestazioni**". Vengono qui illustrati i requisiti relativi al **monitoraggio**, alla **misurazione**, all'analisi ed alla valutazione **dei processi** che hanno un impatto sulla continuità operativa; in particolare vengono esplicitati i requisiti relativi ad **indicatori** e **metriche** finalizzate al monitoraggio della *business continuity*, sempre basandosi sui risultati della valutazione dei rischi.

Nel capitolo 9 vengono anche trattati i requisiti standard per i sistemi di gestione riguardanti gli **audit interni** ed il **riesame del sistema** da parte della direzione. Anche qui, rispetto alle altre normative sui sistemi di gestione, il focus è sui rischi risultanti dal *risk assessment*.

Nel capitolo 10, denominato "**Miglioramento**", sono trattati le **non conformità**, le **azioni correttive** ed il **miglioramento continuo**. Mentre relativamente a non conformità ed azioni correttive la gestione è analoga ai sistemi gestionali descritti nelle normative del passato (ISO 9001 in primis), occorre notare che è scomparso il termine **azione preventiva**, sostituita da tutte quelle azioni che vengono messe in atto al fine di perseguire il miglioramento continuo del sistema e delle sue prestazioni. Premesso ciò, le non conformità relative al sistema di gestione della continuità operative – normalmente **incidenti** ed altre situazioni nelle quali si verifica il non soddisfacimento dei requisiti procedurali – dovranno essere identificate e dovranno essere attuate prontamente correzioni per eliminare, quando possibile, gli effetti della non conformità stessa e le relative conseguenze. Inoltre si deve valutare la necessità di intraprendere azioni correttive finalizzate ad eliminare le cause della non conformità.

In conclusione si tratta di una norma che presenta per la prima volta, insieme alla nuova ISO 27001:2013 appena pubblicata, la nuova struttura delle normative sui sistemi di gestione che ritroveremo nella ISO 9001 del 2015. Evidentemente le organizzazioni che vorranno adeguarsi a tale normativa e certificarsi secondo le proprie esigenze di business, quasi certamente avranno già messo in atto e certificato un sistema di gestione per la qualità ISO 9001, ma probabilmente alcune

di queste organizzazioni avranno anche già implementato il **sistema di gestione della sicurezza delle informazioni ISO 27001**, pertanto lo sforzo per conformarsi a questa norma sulla *business continuity* non sarà eccessivo. Infatti molti requisiti sono comuni fra la norma ISO 22301 e la norma ISO 27001 nella quale esiste già un obiettivo di controllo riguardante la continuità operativa che impone di predisporre uno o più **business continuity plan** per garantire la continuità nell'erogazione del servizio o nella produzione.

Al proposito occorre notare che la norma tratta la gestione di tutti i tipi di discontinuità o interruzioni di servizio, non necessariamente solo quelli legati all'indisponibilità dei sistemi informatici, anche se quasi tutte le organizzazioni vedono come principale pericolo per la propria continuità operativa il blocco dei sistemi informatici che ormai governano quasi tutte le attività aziendali.

Quali saranno, infine, le organizzazioni interessate a certificarsi secondo la ISO 22301? Probabilmente tutte le organizzazioni che operano nel settore dei servizi, anche pubblici, e che devono garantire ai propri clienti una certa continuità del servizio, ovvero banche, assicurazioni, fornitori di servizi in *outsourcing*, fornitori di servizi sul *cloud* ((si veda il [parere della Commissione Europea](#) al riguardo) o comunque servizi Web, fornitori di servizi di assistenza tecnica in settori particolarmente critici.

Le principali normative sull'argomento richiamate esplicitamente o implicitamente da questa norma sono le seguenti:

- ISO 22300, *Societal security – Terminology*
- ISO/IEC 27031, *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*
- BS 25999-1, *Business continuity management – Code of practice*
- BS 25999-2, *Business continuity management – Specification*
- UNI ISO 31000 – *Gestione del rischio – Principi e linee guida*

La continuità operativa per la Pubblica Amministrazione nel Codice per l'Amministrazione Digitale: [vai al sito DIGITPA](#)

Aggiornamento: Oggi disponibile anche in italiano la norma UNI EN ISO 22301:2014 Sicurezza della società – Sistemi di gestione della continuità operativa – Requisiti