Newsletter
n. 8– 2014
Dicembre 2014

BUSINESS CONTINUITY

Care Colleghe, Cari Colleghi,
prosegue la serie delle Newsletter legate agli Schemi di Certificazione di AICQ SICEV esistenti o in fase di costituzione.
Questa volta la "pillola formativa" si riferisce alla "*Business Continuity*" che mi ha messo a disposizione il Dott. Alberto Mattia, *Managing Director* di PANTA RAY, una Società di consulenza e formazione in *Business Continuity & Crisis Management*. Troverete i Suoi riferimenti, in calce all'articolo, che Vi consentiranno di contattarlo qualora necessitiate di chiarimenti e ulteriori informazioni.
PANTA RAY collabora con il *Business Continuity Institute* (BCI) che è l'Organismo leader nel mondo per la continuità operativa. Vi segnalo l'intenzione di AICQ SICEV di aprire, nel 2015, un Registro per la certificazione di Auditor per la *Business Continuity* con la collaborazione di BCI Italian Forum e secondo quanto previsto dalla ISO/IEC 17024.
In questa ottica verrà anche organizzato un seminario sulla *Business Continuity* nell'ambito del programma dei SABATI SICEV.
Buona lettura e buon lavoro.

Roberto De Pari
Direttore AICQ SICEV

Know how in pillole:

Che cosa si intende per ***Business Continuity***?

Per spiegare l'importanza di una materia come la *Business Continuity*, occorre prima comprenderne con esattezza il reale significato. Specialmente in relazione ad altre materie - ugualmente importanti e quindi assolutamente complementari - come il *Disaster Recovery* e il *Risk Management*, con le quali troppo spesso ancora si genera confusione. Quali sono dunque le differenze?

In principio fu l'avvento della tecnologia e la conseguente automazione dei processi a evidenziare nuove criticità da affrontare per garantire il corretto ripristino delle attività in caso di interruzioni. Nasce dunque così il ***Disaster Recovery***, pratica che - in parole molto semplici - progetta ed attua misure finalizzate a garantire il recupero di sistemi, dati e infrastrutture tecnologiche necessarie all'operatività di una Organizzazione. Successivamente, tuttavia, ci si rende conto che - nonostante la forte dipendenza dei processi dalla componente ICT - un'Organizzazione che voglia dirsi realmente resiliente deve tenere in forte considerazione gli impatti di un'eventuale interruzione anche su tutti gli aspetti che esulano dalla tecnologia in senso stretto: risorse umane, organizzazione del lavoro, logistica e commerciale, per citarne solo alcuni. Entra così in gioco il concetto di ***Business Continuity*** che fa leva sulla prevenzione - grazie ad uno degli strumenti principe dell'Organizzazione che è l'analisi d'impatto operativo (Business Impact Analysis) - per garantire sostenibilità e recupero di tutti i processi in caso di interruzione. Le *best practice* in materia si sono poi affinate negli anni, inglobando - specialmente a seguito di episodi di particolare gravità storica come l'11 settembre 2001 -il ***Crisis Management*** all'interno del cosiddetto Sistema di Gestione della Continuità Operativa con lo scopo di portare il processo decisionale al livello strategico di un'Organizzazione (Top Management) in caso di crisi.

Per quanto concerne quindi la relazione tra *Business Continuity* e *Disaster Recovery*, possiamo concludere che quest'ultimo *sia solo una parte – sebbene importante – del Sistema di Gestione della Continuità Operativa*, che però è molto più ampio. Praticare quindi solo il *Disaster Recovery*, non significa avere una solida Business Continuity.

Discorso completamente diverso invece per il ***Risk Management***. Il concetto di rischio, per definizione, è strettamente connesso al calcolo della probabilità che invece ha molto poco a che fare con la *Business Continuity*. I professionisti di continuità operativa sanno bene che in un Piano di Continuità bisogna sempre partire dal presupposto che l'interruzione si possa verificare, a prescindere dalle probabilità di accadimento di un determinato evento avverso. Diverse Società, invece,ancora commettono un errore grossolano e molto

pericoloso, che denota la scarsa cultura in materia presente in Italia: applicano la *Business Continuity* solo al cosiddetto "rischio residuo", ovvero quella parte di rischio che non può essere calcolata, gestita o mitigata. Risultato: quando i modelli matematici su cui si fonda la gestione del rischio sbagliano e non si hanno solide pratiche di continuità operativa incorporate in tutta l'Organizzazione, le medesime incorrono in gravi perdite fino ad arrivare talvolta anche al fallimento.

Pertanto è importante notare come *Risk Management e Business Continuity* siano effettivamente *due materie complementari*: entrambe di fondamentale importanza, ma che non possono e non devono escludersi una con l'altra.

Occorre infine sottolineare come la *Business Continuity* - in italiano **continuità operativa** - non sia una materia riservata esclusivamente ad Organizzazioni private che perseguono un profitto. La confusione in questo caso deriva dalla parola "Business", che viene spesso fraintesa nel contesto italiano poiché richiama concetti meramente affaristici che appaiono però assolutamente riduttivi nella fattispecie della *Business Continuity*. La *continuità operativa*, infatti, *deve essere un'ambizione per qualsiasi Organizzazione* - società private, pubbliche amministrazioni, associazioni no-profit, forze di pubblica sicurezza, ecc. - *che voglia dirsi resiliente e la cui continuità risulti essere necessaria per la solidità e la sostenibilità di un sistema*.

Contesto Normativo

Premesso che la *Business Continuity* deve essere considerata una materia di importanza strategica da applicare in maniera sostanziale e concreta, quindi non come un adempimento meramente formale, è bene sapere che per certi tipi di organizzazioni (pubbliche e private) si tratta anche di un obbligo normativo ben preciso.

A questo proposito occorre citare tre differenti norme:

1. il **Codice dell'Amministrazione Digitale (CAD)** – modificato nell'ultima versione dal Decreto Legislativo n. 235 del 30 dicembre 2010;
2. l'**attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione** – avvenuta mediante Decreto Legislativo n. 61 dell'11 aprile 2011;
3. il **nuovo accordo sui requisiti minimi di capitale** comunemente denominato **Basilea II** del giugno 2004.

CODICE DELL'AMMINISTRAZIONE DIGITALE (CAD)

Si tratta del testo normativo che riunisce i principi alla base dell'amministrazione digitale, modificato e integrato nella sua ultima versione mediante il Decreto Legislativo n. 235 del 30 dicembre 2010 entrato in vigore il 25 gennaio del 2011. Il CAD promuove e regola la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione all'interno della Pubblica Amministrazione e nei rapporti tra amministrazione e privati. Tale Codice ha espresso alcune indicazioni di carattere generale ed altre più specifiche riguardanti il livello minimo di servizio che deve essere garantito al cittadino nei rapporti con la Pubblica Amministrazione. Vi è anche una direttiva ministeriale che definisce criteri e azioni concrete da attuare nelle Pubbliche Amministrazioni per realizzare i principi del CAD. Tale direttiva regolamenta diversi aspetti fondamentali per la continuità dell'attività amministrativa, come ad esempio:

- la comunicazione interna alle Pubbliche Amministrazioni e tra pubblica amministrazione e cittadini;
- le transazioni economiche on-line e la sicurezza dei sistemi informativi in genere;
- le strutture per l'organizzazione, l'innovazione e le tecnologie.

Il CAD non rinnova solamente il quadro normativo in materia di amministrazione digitale aggiornando le regole di riferimento rispetto a un panorama tecnologico in evoluzione. Infatti, è bene notare come esso

introduca anche innovazioni normative che incidono concretamente sui comportamenti, sui processi e sugli aspetti organizzativi delle amministrazioni con lo scopo di migliorare la qualità dei servizi al cittadino attraverso la continuità operativa. Si può quindi concludere affermando che la *Business Continuity* sia dunque un *obbligo inderogabile per la Pubblica Amministrazione*.

DECRETO LEGISLATIVO N. 61 DELL'11 APRILE 2011

Emanato per rendere effettiva l'attuazione della Direttiva 2008/114/CE in materia di individuazione e designazione delle infrastrutture critiche europee e valutazione della necessità di migliorarne la protezione, è entrato in vigore il 5 maggio del 2011. Tale decreto indica inoltre le modalità per la valutazione della sicurezza e le prescrizioni minime di protezione di tali infrastrutture, in conformità a quanto disposto dalla direttiva europea che recepisce. La responsabilità per la protezione delle infrastrutture critiche ricade su diversi soggetti, coinvolti a seconda della loro competenza:

- su territorio nazionale spetta al Ministero dell'Interno, al Ministero della Difesa, al Ministero dello Sviluppo Economico (per il settore energetico) e al Ministero delle Infrastrutture e dei Trasporti (per il settore trasporti), nonché al Dipartimento della Protezione Civile;
- a livello locale la responsabilità è attribuita invece al Prefetto territorialmente competente.

Pertanto, qualora un'infrastruttura venga definita come "critica" secondo i principi emanati a livello europeo si viene a creare una rete di rapporti tra il soggetto pubblico o privato definito come ICE – che dovrà nominare un funzionario di collegamento in materia di sicurezza – e i Ministeri competenti o il Dipartimento di Protezione Civile o la Prefettura per l'analisi dei rischi, la redazione e l'aggiornamento del Piano di Sicurezza dell'operatore. *Piano che dovrà contenere necessariamente tutti gli aspetti relativi alla continuità operativa dell'infrastruttura*, così da garantire un livello accettabile di servizio anche in condizioni di crisi o di emergenze.

NUOVO ACCORDO SUI REQUISITI MINIMI DI CAPITALE - BASILEA II

In vigore dal gennaio 2007, l'accordo sui requisiti minimi di capitale comunemente denominato Basilea II è stato redatto dal Comitato di Basilea per la Vigilanza Bancaria. L'accordo – che preso nella sua interezza è molto ampio e riguarda diversi ambiti del banking – ha tra i principi cardine la gestione dei rischi nell'attività bancaria e la maggiore novità è rappresentata proprio dall'introduzione dei requisiti minimi di capitale a copertura del rischio operativo. E proprio tra i principali fattori di rischio identificati dal Comitato di Basilea vi sono:

- danni a beni materiali (derivanti da atti di terrorismo, vandalismo, terremoti, incendi e inondazioni);
- disfunzioni e interruzioni di natura tecnica.

Inoltre, parallelamente all'emanazione dell'accordo è stato redatto dal Risk Management Group del Comitato di Basilea un documento indipendente intitolato "Sound Practices for the Management and Supervision of Operational Risk" che include 10 principi di gestione del rischio operativo. Il punto numero 7 si concentra proprio sul *contingency planning* e sul Sistema di Gestione della Continuità Operativa soffermandosi sull'importanza dei piani di continuità per garantire costantemente l'erogazione dei servizi e il funzionamento dell'Organizzazione anche in seguito a gravi incidenti o vere e proprie crisi. La *Business Continuity è pertanto un vincolo regolamentare per tutte le banche dei Paesi che aderiscono all'accordo*.

Gli Standard Internazionali dalla BS 25999 alla ISO 22301

La pubblicazione di un primo vero e proprio standard in materia di Business Continuity la si deve al British Standard Institute che nel 2007 ha emanato la Normativa BS 25999 "Specification for Business Continuity

Management", un set di requisiti per l'attuazione, la gestione e l'aggiornamento di un Sistema di Gestione della Continuità Operativa. Con l'introduzione nel 2012 della Normativa ISO 22301 "Societal Security -- Business Continuity Management Systems -- Requirements", tuttavia, tale standard risulta ad oggi superato.

La nuova ISO, infatti, specifica anche le modalità di pianificazione, progettazione, monitoraggio e revisione del programma di gestione della *business continuity*, insistendo sull'importanza di un sistema preventivo che aiuti a ridurre la probabilità di interruzioni, a prepararsi per la risposta a una crisi e al recupero delle attività inteso non solo come mantenimento di un livello minimo accettabile, ma anche come *ripristino del regolare livello di erogazione dei servizi*. Inoltre, la ISO 22301 propone una serie di innovazioni e approfondimenti in materia di continuità operativa che possono essere così riassunti:

- **STRUTTURA**: i requisiti per ottenere la Certificazione ISO sono significativamente di più rispetto a quelli originariamente previsti dalla BS 25999 (105 vs. 56);
- **PIANIFICAZIONE**: riveste un aspetto fondamentale la definizione del perimetro di continuità operativa per l'Organizzazione, per instaurare un Sistema di Gestione che sia rilevante e che effettivamente supporti gli obiettivi societari;
- **LEADERSHIP**: rispetto alla BS 25999, si fa esplicito riferimento al coinvolgimento del Top Management come uno step necessario per la realizzazione di un programma conforme ai dettami della ISO;
- **COMUNICAZIONE**: viene posta molta enfasi sull'importanza delle comunicazioni interne ed esterne verso le parti interessate (media, forze di pubblica sicurezza, autorità, clienti, fornitori, ecc.), sia in caso di interruzione che in condizioni di regolare operatività;
- **DEFINIZIONE E MISURAZIONE DEGLI OBIETTIVI**: le performance di continuità operativa devono essere monitorabili e misurabili per fornire una valutazione di merito circa le performance e l'efficacia del programma di gestione della continuità operativa.

I requisiti previsti dalla ISO 22301 sono comunque estremamente generici, come tipico di ogni standard che si proponga come punto di riferimento per Organizzazioni di diversi settori, dimensioni e scopi.

Certificazioni Professionali - Il Ruolo del Business ContinuityInstitute

Il *Business Continuity Institute* (BCI, www.thebci.org) è l'organismo leader nel mondo per la continuità operativa. Fondato nel 1994, il BCI è oggi riconosciuto come il più importante ente di certificazione per i professionisti di business continuity a livello globale grazie al suo programma di formazione intensivo in 5 giornate basato sulle **Good Practice Guidelines** emanate nel 2013 e ispirate a loro volta alla ISO 22301 sopra menzionata.

Il BCI offre una vasta gamma di risorse per i professionisti che si preoccupano di aumentare il livello di resilienza delle proprie Organizzazioni o che intendono considerare una carriera nell'ambito della continuità operativa. Con oltre 8.000 membri all'attivo che lavorano in circa 3.000 Società dei settori privato, pubblico e no-profit in più di 100 Paesi nel mondo, il BCI si impegna nella ricerca dell'eccellenza nella *business continuity* e i suoi titoli statutari sono da sempre garanzia di competenza tecnica e professionale nella continuità operativa.

IL BUSINESS CONTINUITY INSTITUTE IN ITALIA

In agosto 2014 il Business Continuity Institute ha nominato il - BCI Italian Forum Leader (Gianna Detoni) con l'obiettivo di costituire e sviluppare il primo network italiano targato BCI di professionisti con competenze certificate in materia di continuità operativa (BCI Italian Forum, www.thebci.it). Il forum è la piattaforma (assolutamente gratuita) attraverso la quale i professionisti hanno occasione di confrontarsi sulle tematiche di fondamentale importanza inerenti la continuità operativa. Il fine è quello di far crescere la consapevolezza

sull'argomento in modo da condividere metodologie, esperienze e *best practice* in materia di *Business Continuity*. Un'opportunità per elevare il livello della continuità operativa in Italia mediante la diffusione di una cultura della prevenzione e della pianificazione delle strategie di recupero da un incidente. Il forum rappresenta quindi l'occasione per colmare il gap accumulato verso alcuni Paesi esteri (in particolare quelli anglosassoni), allineare le Organizzazioni locali alle *best practice* in materia e per promuovere la certificazione delle competenze professionali e tecniche necessarie per il rispetto della Norma ISO 22301:2012 e delle normative nazionali e internazionali.

ALBERTO MATTIA
Managing Director di PANTA RAY (www.pantaray.eu) - Società di consulenza e formazione specializzata in Business Continuity & Crisis Management
Segretario Generale dell'Associazione HI CARE (www.hi-care.eu)
mattia@pantaray.eu