CRISIS MANAGEMENT

Manuale di business continuity e crisis management

La gestione dei rischi informatici e la continuità operativa

NUOVA EDIZIONE AGGIORNATA

Anthony Cecil Wright

FRANCOANGELI

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con

La versione completa dell'e-book (a pagamento) è leggibile con Adobe Digital Editions. Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta cliccando qui le nostre F.A.Q.

Am - La prima collana di management in Italia

Testi advanced, approfonditi e originali, sulle esperienze più innovative
in tutte le aree della consulenza manageriale,
organizzativa, strategica, di marketing, di comunicazione,
per la pubblica amministrazione, il non profit...

Anthony Cecil Wright

Manuale di business continuity e crisis management

La gestione dei rischi informatici e la continuità operativa

NUOVA EDIZIONE AGGIORNATA

FRANCOANGELI

Grafica della copertina: Elena Pellegrini

Indice

Ringraziamenti

Ritengo questa pagina importante, non trattando aspetti tecnici, ed essere la parte più complicata del testo, in quanto temo di scordarmi qualcuno di importante, ma anche di non essere capace di esprimere bene il mio pensiero.

Chiedo, quindi, scusa in anticipo.

Innanzitutto, dedico questo libro al collega Andrea Moccia che mi ha dato in banca una grande mano nella realizzazione dei BCP del Gruppo.

Un grazie a Lorena Gambini, Stefano Sarni, ad Andrea Beretta e ai suoi fantastici colleghi, che hanno vissuto con me quel periodo assai "caldo"! (E che mi hanno sopportato!).

Un ringraziamento particolare alla "squadra" IBM, la cui elevata competenza e disponibilità permise alla banca anche di migliorare continuamente i livelli di servizio.

Un grazie a Mario Sestito con il quale, in questi ultimi anni, ho instaurato uno scambio di vedute assai produttivo sui temi che ci occupano (lui è l'esperto in business continuity e information security) e un grazie ai suggerimenti che mi ha dato. Assieme a lui, un grazie anche a Vincenzo Giardina, altro grande esperto in business continuity.

Un ringraziamento alla dr.ssa Clara Salpietro, giornalista coraggiosa (sempre presente nei territori di guerra), sensibile e generosa, per il suo aiuto nella parte del testo relativa al crisis management.

Last but not least, un grazie alla dr.ssa Ilaria Angeli per la fiducia accordatami. Sono affezionato alla Casa Editrice: infatti fu proprio da un breve incontro con suo padre, Franco Angeli, che nacquero i libri che poi ho scritto. Il primo, ben quarant'anni fa!

ACW

Introduzione

1. Elementi caratteristici di rilievo del testo

Ho voluto chiamarlo "manuale" per diverse ragioni fondamentali:

- deve essere di pronto utilizzo, specialmente per chi opera da tempo nell'informatica e nell'organizzazione;
- deve essere il frutto dell'esperienza maturata in diversi anni e in settori economici differenti;
- deve essere il più completo possibile, in base alle conoscenze e alle opinioni di autorevoli organismi internazionali (infatti, vi sono riferimenti a degli standard internazionali in materia, alla normativa di vigilanza per le banche e le assicurazioni, ad alcuni testi, ecc.);
- deve però anche introdurre progressivamente nella materia chi affronta questi temi per la prima volta;
- l'esposizione deve essere la più chiara possibile, in modo da facilitarne l'immediata comprensione;
- deve essere equilibrato nel livello di profondità: sintetico, ove è orientato a dare una risposta immediata ed esauriente a degli aspetti tecnici (mi immagino colui o colei che sono impegnati in un progetto di business continuity e vogliono capire come orientarsi per raggiungere un determinato obiettivo); opportunamente sviluppato, ove si tratti di introdurre il Lettore a un tema nuovo o molto poco conosciuto (ad esempio, che cosa sono: la business continuity e in cosa consiste; il risk management e il rapporto con la business continuity; la sicurezza della supply chain; aspetti di sicurezza nell'esternalizzazione di processi vitali o critici; ecc.).

Questo testo, nelle mie intenzioni, dovrebbe rispondere a tutti i sopra riportati obiettivi.

Ovviamente la risposta è al Lettore!

2. Fonti

Nel testo trasferisco metodi, accorgimenti, tecniche e suggerimenti derivanti dalla mia esperienza diretta in una grande azienda per 24 anni; quindi, successivamente, facendo consulenza a diverse aziende ed organizzazioni. Per ragioni di completezza informativa, come accennato negli obiettivi di questo testo, faccio riferimento anche al contenuto di pertinenti standard internazionali o all'opinione espressa da importanti istituzioni, quali la Banca d'Italia, o istituti, quali il Business Continuity Institute.

In questo modo, il Lettore, detto in poche parole, ottiene delle linee guida frutto di un "matrimonio" fra esperienza e metodologie riconosciute a livello mondiale.

3. Consigli per il Lettore

Il testo è stato concettualmente e sostanzialmente diviso in due parti: ciò ai fini di introdurre gradualmente il Lettore alle tematiche trattate.

La prima è di introduzione alle metodologie necessarie a rendere un'organizzazione più resiliente, fornendo una visione a "volo d'uccello", ma sufficiente per gli scopi di chi deve introdurre e manutenere in un'organizzazione i processi di business continuity.

Infatti, si entra gradualmente nello "spirito" della business continuity e si affrontano gli argomenti e i metodi più importanti ad essa connessi.

In questa prima parte ho inserito quei concetti che, a mio parere, se illustrati nel corso della descrizione dettagliata di come operare per rilevare i dati e per progettare i piani di continuità, avrebbero eccessivamente interrotto il flusso della disamina.

Una volta che il Lettore ha compreso la "filosofia" di base, gli scopi e argomenti quali il come si inserisce la business continuity nell'ambito del global risk management, la rilevanza della filiera produttiva, l'outsourcing, ecc., secondo me è facilitato nell'apprendere il cosa fare.

Nella seconda parte, infatti, si entra nel "vivo" affrontando in dettaglio il "cosa fare" per ottenere dei piani di continuità e di gestione dell'emergenza, in linea con l'esperienza e gli standard internazionali.

Il Lettore completamente "a digiuno" sui temi trattati potrebbe trovare alcuni concetti della prima parte leggermente non intuitivi: non si deve preoccupare perché la risposta ai suoi interrogativi la troverà sicuramente più avanti nel testo.

Il mio approccio, infatti, è per "approssimazioni successive", da una "vista dall'alto" ad un successivo maggiore dettaglio e, se necessario, l'inserimento più avanti di un altro concetto correlato.

Vi sono anche esempi sia orientati ad illustrare quanto detto, sia a far entrare progressivamente il Lettore nell'argomento trattato.

Non ultimo, alcuni esempi illustrano l'ambiente lavorativo, utile per chi ancora deve affrontare questa esperienza.

Fra questi esempi vi è un case study ("l'artigiano di qualità") che è citato a più riprese, man mano che vado in profondità: l'esempio è facilmente comprensibile dato che tratto la lavorazione di cravatte da parte di un artigiano in un negozio e, quindi, il Lettore non è distratto da procedure operative che non conosce (cosa che probabilmente avverrebbe se si parlasse di investimenti finanziari o di gestione degli ordini di acquisto e vendita) e può capire i suggerimenti e le osservazioni che ho scritto.

Quindi: buona lettura!

4. La suddivisione

Ai fini di far entrare progressivamente il Lettore nell'argomento principe, desidero mettere sul "piatto" i principali argomenti di cui ci occuperemo abbondantemente nel corso del testo.

4.1. Prima parte

La finalità della prima parte (primi otto capitoli) è quella di iniziare a far comprendere al Lettore:

- cosa si intende per business continuity;
- l'esame della filiera produttiva: dalla logistica all'outsourcing;
- quali le origini e le evoluzioni;
- quali sono gli obiettivi della business continuity oggi;
- in cosa consiste il risk management e quali tecniche si possono utilizzare;
- il rapporto fra risk management e business continuity;
- l'identificazione dei processi critici;
- quali le possibili difficoltà che si incontrano, ma anche quali "facilitatori" utilizzare;
- quali standard internazionali trattano la business continuity e temi ad esso correlati (ad esempio il disaster recovery);
- in cosa consistono le nuove norme di vigilanza prudenziale emanate dalla Banca d'Italia e perché è importante conoscere la loro esistenza;

- come agisce anche un'altra istituzione finanziaria importante, non europea, quale la Monetary Authority of Singapore[1];
- come è strutturato lo standard che tratta la business continuity dei processi critici e quello che include le norme per la protezione dei dati dal rischio di indisponibilità;
- quali le competenze e conoscenze richieste al professionista della business continuity e al business continuity manager.

Potremmo dire che, in buona sostanza, questa prima parte tratta del "come fare".

4.2. Seconda parte

Dal capitolo 9 il Lettore entra nel "cosa fare". La suddivisione dei capitoli è in linea con le principali fasi progettuali:

- la preparazione al progetto;
- la raccolta dei dati e la loro valutazione;
- la formulazione delle ipotesi di trattamento;
- il disegno e stesura dei piani di continuità;
- la verifica di funzionamento dei piani;
- come organizzarsi per la gestione degli incidenti e delle emergenze;
- come evitare una possibile emergenza e, qualora dovesse purtroppo avvenire, come gestirla al meglio;
- il rientro alla normalità dopo un disastro;
- la documentazione da produrre e da conservare.

5. Avvertenze relative alla nuova edizione

Tra il 2018 ed il 2019 sono stati pubblicati gli aggiornamenti di alcuni importanti standard ISO. Fra questi, ci interessa l'aggiornamento nel 2019 dello ISO/IEC 22301. Una variazione leggermente significativa è rappresentata dalla non menzione di due indicatori (RPO, MBCO) molto utili nella didattica; ho deciso però, essendo rimasto il concetto, di lasciare i nomi.

[1] Ho voluto fare riferimento a questa istituzione sia perché è a mio parere la più severa a livello internazionale, sia in quanto molte grandi imprese italiane sono impegnate in quella Nazione.

1 Che cosa è la “business continuity”?

1. Definizione

Da buon manuale, deve rispondere con una definizione generalmente accettata. Eccola:

> business continuity: capacità di una organizzazione di continuare a fornire i servizi e prodotti in intervalli di tempo accettabili ad una capacità predefinita a seguito di un disastro[1].

Gli americani, invece, danno una definizione[2] più tesa ad indicare ciò che va fatto, ossia

> un processo continuo finalizzato ad assicurare che siano presi gli opportuni passi atti ad identificare la severità delle possibili perdite e a mantenere strategie praticabili per la ripresa dell’operatività e la continuità dei servizi.

Come si vede, si definisce la business continuity un processo continuo, cosa che in effetti è, come vedremo più avanti.

Possiamo, da queste definizioni, comprendere quale sia la finalità: far sì che un’organizzazione sia resiliente[3], in grado cioè di poter continuare a pro-

[1] In inglese: “capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption”. Nel testo ho riportato una mia libera traduzione.

[2] Lo standard NFPC 1600 così la definisce: “Business continuity. An ongoing process to ensure that the necessary steps are taken to identify the impacts of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services”.

[3] Resilienza: in ingegneria è la capacità di un materiale di resistere a forze impulsive (ovvero, della capacità di resistere ad urti improvvisi senza spezzarsi; liberamente tratto da Wikipedia).

durre e a servire i clienti malgrado sia stata oggetto di un evento che ne ha compromesso in maniera più o meno grave la capacità di proseguire il suo business e le sue attività al livello usuale.

Come si nota dalla definizione dell'ISO 22301, non si parla di continuare come se "nulla fosse accaduto", bensì di continuare a un livello predefinito, ritenuto accettabile.

È chiaro che, una volta gestito l'incidente, il passo successivo è quello di cercare di riprendere l'attività normale in tempi "ragionevoli".

Da questa definizione e da queste considerazioni, si capisce che ciò che un'organizzazione deve valutare e stimare sono, tra gli altri, i valori da assegnare al cosiddetto "livello accettabile" e a "tempi ragionevoli", citati dallo standard.

Il primo valore dipende dalla dimensione dell'incidente e dai costi da sostenere per far sì che, qualunque sia la dimensione del disastro, l'operatività prosegua possibilmente a un livello predefinito "accettabile".

Come vedremo nei prossimi capitoli, si devono stimare le risorse da impiegare per le misure preventive da adottare e per la ripresa dell'attività in emergenza, e compararle rispetto ai benefici, diretti e indiretti, derivanti dalla prosecuzione delle attività. Qualora i costi siano superiori ai possibili benefici, l'organizzazione può eventualmente decidere di accettare il rischio oppure di trasferire il rischio a terzi. Quali sono i "tempi ragionevoli" di ripartenza?

Senz'altro sono stimati sulla base della perdita economica che si verificherebbe al prolungarsi del tempo di disservizio. Più dura il disservizio, maggiori sono le conseguenze e quindi i costi subiti. Tali valori saranno ottenuti tramite interviste agli addetti ai lavori.

È importante che l'azienda[4] valuti i possibili rischi e prenda conseguentemente una decisione attentamente valutata.

1.1. Un po' di storia: le origini della business continuity

Senz'altro, nei primi tempi, e mi riferisco agli anni '90 e primi anni 2000, l'ottica della continuità operativa era concentrata sulla disponibilità dei propri sistemi informatici e informativi, tant'è vero che si parlava di "disaster recovery", ossia della possibilità di garantire la disponibilità delle applica-

[4] Qui cito il termine "azienda", ma avrei potuto dire: ente, istituzione, ministero, ecc. In generale, farò uso nel testo del termine "organizzazione": ciò in quanto quello che dico è valido per qualsiasi tipo di organizzazione. A volte, onde non ripetere la stessa parola, cito i termini azienda o impresa.

zioni e dei dati, anche in caso di grave disastro al computer o al centro elettronico primario.

Ciò avveniva mediante la conservazione dei dati e dei programmi su supporti magnetici (in genere su nastri magnetici, dato il minor costo per gigabyte rispetto ai dischi); questi venivano raccolti in appositi armadi ignifughi o nello stesso stabile o anche in un altro sito.

Nei primissimi tempi, dato che l'informatica (fatta eccezione per le aziende di produzione ove i computer governavano le macchine) era impiegata principalmente per meccanizzare delle operazioni manuali, e gli addetti avevano le competenze per proseguire le attività a mano, in caso di assenza del computer, l'eventuale distruzione o non utilizzabilità del computer era affrontata facendo accordi con terze parti per l'uso della loro potenza elaborativa all'occorrenza. I tempi di ripartenza erano spesso stimati in giorni.

Successivamente, a seguito di incendi (anche operati da gruppi terroristici) di alcuni ambienti lavorativi, fra i quali i centri elettronici, le copie giornaliere dei dati su nastro furono portate a una distanza adeguata dal centro elettronico, e molte aziende (soprattutto le banche) costruirono dei centri elettronici di backup.

Ricordo, a questo proposito, che la BNL agli inizi degli anni '80 aveva tre centri elettronici: due a Roma (Centro Regionale per il Centro Sud e il Centro Nazionale) e uno a Milano (Centro Regionale per il Nord) e copie dei nastri del centro nazionale di Roma venivano giornalmente inviate a Milano. In questa città, venivano conservate tre copie: quella del giorno X-2, quella di X-1 e quella del giorno X. Quando arrivava la successiva copia, la oramai vecchia copia del giorno X-2 (chiamata simpaticamente del "nonno") veniva riportata a Roma e i relativi nastri venivano riutilizzati per la copia dei nuovi "figli".

Se non erro, è intorno al 1994-1995 che si incomincia a parlare proprio di business continuity, e quindi a prendere in esame non solo il sistema informativo ma anche tutto ciò che serve per poter proseguire nell'attività istituzionale dell'organizzazione (prevalentemente uffici e attrezzature). È in quell'epoca che nasce il Business Continuity Institute in Gran Bretagna.

Pur tuttavia, non mi risulta che la gran parte delle aziende eseguisse delle prove di ripartenza con le copie di backup da un altro centro elettronico. Chi eseguiva delle prove, le faceva parziali; ad esempio, veniva provata la possibilità di far ripartire una singola procedura, quella più importante.

Inoltre, le organizzazioni, fatta eccezione per il settore della difesa e le multinazionali con forti investimenti nella ricerca e sviluppo di prodotti, non si preoccupavano di verificare la capacità di poter proseguire l'attività istituzionale in caso di un disastro che colpisse le infrastrutture e soprattutto le persone chiave.

La vera svolta, a mio parere, è avvenuta quando si sono riesaminati gli accadimenti drammatici dell'11 settembre 2001. In quell'occasione, più che l'indisponibilità dei centri elettronici primari, di backup (alcuni avevano questi centri nella seconda torre data l'assenza di probabilità che entrambe potessero crollare!) e degli uffici con relativa documentazione cartacea, si ebbe purtroppo una perdita elevata di vite umane.

La scomparsa di tante persone "chiave" per il business, in un colpo solo, non si era mai verificata prima di allora[5].

Box 1 – Lezioni apprese dalla tragedia dell'11 settembre 2001

A parte le considerazioni, che qui non andiamo a riprendere, relative alle carenze organizzative nell'ambito del coordinamento degli interventi da parte delle istituzioni americane (chi chiamava per il soccorso riceveva risposte contraddittorie o addirittura errate), e alla non conoscenza dei piani di emergenza da parte delle persone operanti nelle due torri, il rapporto finale della commissione nazionale americana sugli attacchi terroristici evidenzia in particolare che il settore privato controlla l'85% delle infrastrutture critiche di una nazione; pertanto afferma[6]:

certamente, a meno che l'obiettivo dei terroristi sia militare o di un altro sito governativo, i primi ad essere coinvolti sono sicuramente i civili. La sicurezza della nazione ("homeland security") e la preparazione nazionale iniziano proprio con il settore privato.
La preparazione nel settore privato e quello pubblico per il salvataggio, la ripresa, la continuità delle operazioni, dovrebbe includere (1) un piano per l'evacuazione, (2) adeguate capacità di comunicazione, e (3) un piano per la continuità delle operazioni.
Mentre esaminavamo la risposta di emergenza all'11 settembre, testimoni dopo testimoni ci hanno riferito che, malgrado sia avvenuto il disastro del 9/11, il settore privato rimane largamente impreparato di fronte a un attacco terroristico.
Siamo stati anche avvisati che la mancanza di uno standard largamente accettato dal settore privato è il principale fattore che contribuisce a questa mancanza di preparazione.
Abbiamo risposto a queste considerazioni chiedendo all'American National Standards Institution (ANSI) di sviluppare un condiviso standard nazionale per la preparazione [all'attacco] finalizzato al settore privato.

Fu così che negli USA fu redatto e pubblicato lo standard NFPA 1600, lo *Standard on Disaster/Emergency Management and Business Continuity Programs*, aggiornato successivamente nel 2013.

[5] Morirono oltre 2.000 persone impiegate negli uffici. Per fortuna, oltre 16.000 si salvarono.

[6] È anche questa una mia libera traduzione tratta dal testo *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (2004, authorized edition, Norton & Company).

In Inghilterra fu emanato lo standard BS 25999 che è rimasto, fino a maggio 2012, lo standard più utilizzato per la certificazione delle persone e delle aziende alla business continuity. Altre nazioni quali l'Australia, Giappone, Israele e Singapore hanno pubblicato analoghi standard.
Tutto ciò è avvenuto tra il 2004 e il 2007.
A maggio del 2012, la International Standard Organization ha pubblicato lo standard 22301 che, pertanto, costituisce ora il principale riferimento a livello mondiale. Nel 2019 sono state apportate alcune modifiche.
Diversi sono i punti di contatto tra questo standard e il BS 25999.

Altra evidenza da ricordare, dato il caos[7] che si creò in quel tragico giorno, è stata la constatazione amara che se non si fanno periodicamente le prove dei piani di emergenza, al momento della necessità si fanno troppi errori che, a volte, si pagano assai cari.

Le prove, coinvolgendo le persone, fanno sì che oltre a verificare la bontà dei piani stessi, le persone apprendano quali sono le istruzioni da seguire e se le ricordino al momento opportuno.

Tutti aspetti importanti che si ritrovano negli standard di sicurezza sviluppati successivamente.

Continuità operativa

In italiano, come si è notato, ho chiamato la business continuity con la seguente dizione: "continuità operativa".
Credo che detta dizione fu utilizzata la prima volta in un primo documento redatto dalla Banca d'Italia nel luglio 2004 (linee guida alla continuità operativa), documento nel quale venivano fissate delle norme di vigilanza prudenziale nei riguardi delle banche e degli operatori del sistema finanziario italiano, ai fini di aumentarne la resilienza dopo i noti fatti dell'11 settembre[8,9].
Pertanto, userò indifferentemente sia "business continuity management" sia "continuità operativa" per significare entrambe le cose.

[7] Molte persone si sarebbero potute salvare qualora avessero saputo che le porte del tetto erano chiuse a chiave e che si dovevano scendere le scale; infatti per un certo tempo la scala "A" della prima torre colpita rimase praticabile.

[8] A luglio 2013 la Banca d'Italia ha emanato delle nuove norme che hanno sostituito quelle redatte in precedenza a luglio 2004: aggiornamento n. 15 alla circolare 263/2006 *Norme di Vigilanza Prudenziale*; d'ora in poi da me citato come "agg.to n. 15".

[9] "Gestione della continuità operativa: insieme delle iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti o catastrofi che colpiscono direttamente o indirettamente un operatore" (Banca d'Italia, *Nuove norme di vigilanza prudenziale per le banche*, agg.to n. 15).