MANAGEMENT

La resilienza organizzativa

Come gestire i cambiamenti mediante gli standard internazionali

Anthony Cecil Wright

FRANCOANGELI

FrancoAngeli
Edizioni La passione per le conoscenze

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con **Adobe Acrobat Reader**

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

La resilienza organizzativa

Come gestire i cambiamenti mediante gli standard internazionali

FRANCOANGELI

Indice

Ringraziamenti pag. 9

Prefazione, di *Luigi Di Marco* » 11

Introduzione » 13

1. Risk management, business continuity o resilienza organizzativa? » 15

1.1. Rischio e resilienza: introduciamo il tema » 15

1.2. Le vulnerabilità » 18

Penetration test: nulla di nuovo? » 24

Negli ultimi anni qualcosa sta cambiando (in meglio?) » 27

Il “cigno nero”: episodi veramente tali o invece prevedibili? » 31

La funzione aziendale di enterprise risk management » 33

From just-in-time to just-in-case? » 40

1.3. La compliance » 49

Elementi di ISO 37301 – Compliance management systems – Requirements with guidance for use » 52

1.4. Riassumiamo » 60

2. Le aziende e lo standard ISO 22316 » 62

2.1. Le aziende stanno già investendo in resilienza organizzativa? » 62

Riassumiamo » 73

2.2. La resilienza » 73

2.3. Lo standard ISO 22316 – Sicurezza e resilienza – Resilienza organizzativa – Principi e attributi pag. 78
La struttura » 78
I principi » 80
Il coinvolgimento del personale » 81
Prepararsi agli eventi disastrosi » 84
Sintonia fra management e personale » 86
Gli attributi » 87
Quali i riferimenti per le discipline gestionali da coinvolgere? » 91
Misurazione e monitoraggio » 94
Eliminare le cause delle vulnerabilità riscontrate ed elencate in precedenza » 96
Il personale » 97
2.4. Cenni di evoluzione storica della resilienza » 101
2.5. I management system » 103

3. Le discipline gestionali » 106

3.1. Il risk management e lo standard ISO 31000 – Risk management – Guidelines » 106
Introduzione » 106
I principi » 108
Il framework » 109
I processi » 111
Il perimetro » 112
Il contesto » 112
I criteri di rischio » 113
Risk identification » 114
Quali tecniche si possono utilizzare? Cosa afferma l'ISO 31010 – Risk management – Risk assessment techniques » 117
Risk analysis » 123
Risk evaluation » 123
Risk treatment » 123
Monitoraggio, revisione, documentazione » 124

Riassumiamo pag. 124
3.2. La governance dell'IT – Cenni allo standard ISO/IEC 38500 » 125
3.3. Introduzione ai sistemi di gestione e alle discipline gestionali » 128
La struttura » 128
Il contesto dell'organizzazione » 133
Leadership ed emanazione della policy » 138
Ruoli e responsabilità » 143
3.4. Le esercitazioni: breve esame dello standard ISO 22398 » 146
Pianificazione del progetto » 150
Il supporto » 152
Prime conclusioni » 153
3.5. La clausola 8 operations degli standard ISO per i sistemi: ISMS, BCMS, SMS » 155
ISMS » 155
BCMS » 158
SMS » 161
Valutazione delle prestazioni » 163
Miglioramento continuo » 163
4. Considerazioni finali » 165
4.1. Un nuovo approccio » 165
Quali risultati e attività richiede l'ISO 22316 » 166
Come procedere? » 168
Capire » 169
Raccogliere informazioni sulle discipline gestionali » 169
Decidere quali obiettivi si desiderino e con quali tempistiche » 170
Pianificare il progetto o il programma di progetti realizzativi » 170
Bibliografia » 173
Documenti citati » 175

Ringraziamenti

Desidero ringraziare coloro che mi hanno fornito molti utili suggerimenti.

Elisabetta Nori: il suo commento positivo, dopo aver letto il mio testo, è stato un momento di grande sollievo per me, dato che esso proveniva da una persona con profonda conoscenza e una lunga esperienza nell'enterprise risk management. In aggiunta, anche grazie al suo incarico nell'associazione dei risk manager, ERMINE, partecipa ai dibattiti e studi sul tema della resilienza che vedono coinvolti esperti di lunga data e di prestigiose università. La ringrazio di cuore per i suggerimenti forniti.

Mario Sestito: il suo parere e i suoi consigli erano anch'essi un requisito indispensabile per decidere se proseguire nel finalizzare il testo e inviarlo alla casa editrice. Infatti, Mario ha un'esperienza pluridecennale nell'area dell'information security e della business continuity. È certificato ai principali standard ISO da me menzionati e nel suo curriculum vanta anche l'aver ottenuto la certificazione di ICCREA all'ISO 27001 e ISO 22301. Nell'ultimo periodo ha ricoperto anche responsabilità nell'operational risk management. Lo ringrazio caldamente.

Giovanni De Cindio: la sua lunghissima esperienza da economista e statistico è stata preziosa per correggere alcune mie imperfezioni nell'impostazione e per i suoi suggerimenti. Gliene sono grato.

Un ringraziamento a parte merita un grande maestro: **Luigi Di Marco**. Lo ringrazio per le stupende parole, che riporto nell'acclusa Prefazione, ma soprattutto perché il suo parere positivo a quanto da me esposto mi ha dato serenità. Non esagero: chi scrive un testo scientifico, nel quale esprime il suo pensiero, non può essere tranquillo e certo di aver saputo spiegare il proprio messaggio finché una persona autorevole non lo tranquillizza. Grazie maestro.

Prefazione

di Luigi Di Marco

Un uomo colto mi ha chiesto di presentare, dal mio punto di vista, il manuale da lui confezionato e proposto per la stampa e diffusione all'editore.

Ho cominciato a sfogliare le oltre centocinquanta pagine e ho fatto subito ritorno alla prima pagina ove l'autore traccia i comportamenti che intende tenere e suggerire.

L'ordine mentale con cui il testo espone le varie tematiche rende l'operatore, che ne è utilizzatore, capace di agire in ogni situazione problematica.

Il protagonismo dei vari soggetti chiamati in causa è rafforzato da questo manuale che diviene un valido supporto in ogni situazione.

A titolo di esempio riporto: "la resilienza organizzativa è la capacità di un'organizzazione di assorbire e adattarsi in un ambiente in evoluzione per consentirle di raggiungere i propri obiettivi, sopravvivere e prosperare".

Il testo in scioltezza prosegue cavalcando vari temi e problemi.

L'autore gioca con realismo e rispetto con le terminologie anglofone, ma le rende agili e chiare anche per imprenditori e manager inesperti.

Continua con leggerezza commentando libri e contributi a tutto giro, facendo di questo manuale un'opera unica.

Essa affronta la vasta materia trasformando i vari argomenti assimilandoli alla complessa struttura di un pianoforte, i cui tasti rappresentano le varie problematiche aziendali. L'imprenditore e/o il manager rappresentano i pianisti che usano il manuale come uno spartito.

La musica aziendale diviene armonia.

Introduzione

Il testo si apre con gli eventi disastrosi che stanno sempre più colpendo tutte le organizzazioni, anche le più sensibili alla protezione degli asset e alla continuità del business.

Ciò che è sempre più ribadito dalla stampa, nei convegni, negli studi universitari, è che avvengono sempre più frequentemente gravi eventi disastrosi non prevedibili o estremamente rari.

Queste organizzazioni ben strutturate nella maggior parte dei casi seguono i più diffusi standard e framework internazionali (ISO 9001, ISO/IEC 27001, ISO 22301, NIST, COBIT, ITIL ecc.)[1] e si sottopongono a periodici audit onde verificarne la conformità.

Se sono strutture critiche per la nazione (sanità, telecomunicazioni, trasporti, acqua, energia, finanza, difesa) rispettano apposite normative stringenti.

Eppure, leggiamo sui giornali che tante aziende, enti e imprese sono state colpite da un grave disastro (per un evento naturale, o un attacco cyber, o per frode interna ecc.) e hanno sofferto interruzioni prolungate nel servizio, perdite economiche elevatissime, e hanno spesso persa la reputazione e l'immagine.

Ciò che sta emergendo negli ultimi anni è *che la conformità agli standard e framework è una condizione necessaria per essere resilienti, ma non è sufficiente***.** Possono costituire, se ben utilizzati, la base per ottenere la resilienza[2], ma serve un'adeguata cultura organizzativa[3] che consenta di gestire e possibilmente anticipare i cambiamenti.

[1] Per maggiori indicazioni sui documenti citati consultare la bibliografia.

[2] Quando cito la parola resilienza, ed è chiaro dal contesto, intendo "resilienza organizzativa".

[3] È definita come: insieme di convinzioni, valori, attitudini e comportamenti di un'organizzazione, i quali contribuiscono allo specifico ambiente sociale e psicologico nel quale opera.

Si esamineranno, brevemente, le lezioni apprese dalla recente estesa pandemia di SARS-Cov-2: evento di per sé prevedibile, ma non per la durata e l'estensione che ha provocato uno scenario globale disastroso e sarà ricordato per decine di anni. Si citeranno le esperienze di tante organizzazioni, cogliendo le loro esperienze e lezioni apprese attraverso le relazioni e studi di primarie società e università. Si potrà vedere come, partendo dalle principali e più diffuse vulnerabilità e dai suggerimenti di un apposito standard internazionale (ISO 22316)[4], un'organizzazione possa migliorare la sua resilienza. Lo standard però non indica come applicarlo praticamente.

Questo testo è un "manuale", in quanto mira proprio a fornire indicazioni pratiche sull'applicazione dei principi di resilienza organizzativa: ciò direttamente a tutti coloro che, indipendentemente dalla specializzazione, sono interessati a capire e a far sì che la propria organizzazione sia in grado di "assorbire e adattarsi in un ambiente in evoluzione, al fine di consentirle di raggiungere i propri obiettivi e sopravvivere e prosperare". Come afferma lo standard.

[4] Cfr. SO 22316, Security and resilience – Organizational resilience – Principles and attributes.

1 Risk management, business continuity o resilienza organizzativa?

1.1. Rischio[1] e resilienza: introduciamo il tema

Questo libro vuole essere un vero manuale e quindi una "cassetta degli attrezzi" utile per tutte le aziende e gli enti nel prepararsi a eventi disastrosi estremamente rari o non accaduti fino a ora, in modo da ridurne le conseguenze e ritornare all'usuale e desiderata operatività nel più breve tempo possibile. Cercherò di illustrare come un'organizzazione può operare per mettere in atto quei meccanismi che sono necessari per assorbire e adattarsi rapidamente in un mondo che cambia.

Si parla di resilienza e in particolare di resilienza organizzativa da molti anni, ma spesso con indicazioni operative fra loro anche divergenti.

Alcuni testi più noti mettono una forte enfasi sulla *business continuity*, quasi a voler indicare in questa metodologia la soluzione corretta in quanto meglio interpreta le esigenze di essere resilienti.

La business continuity, che illustrerò più avanti nel testo, ha il vantaggio di far ragionare su eventi rari ma disastrosi per ampiezza e durata e far predisporre degli opportuni piani da attivare qualora l'incidente si avveri. Fra gli aspetti positivi vi è il fatto che non sono richiesti investimenti consistenti a priori, in quanto la metodologia prevede che l'organizzazione possa valutare l'opportunità di sostenere i costi, che potrebbero anche essere di una certa rilevanza, solo qualora si dovesse verificare la temuta minaccia; infatti, la necessità di investimenti in misure preventive elevate è oramai estremamente rara, anche in considerazione dell'offerta di servizi in cloud. Normalmente, ciò che viene richiesto è la stesura di piani di continuità e la pianificazione delle relative esercitazioni sul loro funzionamento.

[1] "Risk: effect of uncertainty on objectives" (Rischio: effetto dell'incertezza sugli obiettivi) (ISO31000).

I team di business continuity si pongono questa domanda: "Qualora dovesse avvenire l'incidente o il disastro in esame, e dovessimo perdere la disponibilità di questi dati o asset per un periodo prolungato, che impatto economico, o legale, o reputazionale, potremmo avere? Lo potremmo accettare?". Se la risposta è negativa, allora l'organizzazione deve studiare come poter reagire.

La metodologia si basa su una serie di presupposti, su elementi e fattori che non sono facilmente reperibili nelle organizzazioni. Si richiede un ambiente in grado di assistere il responsabile della business continuity nell'identificazione dei rischi, nell'apprendimento dei criteri di rischio formalmente accettati dall'organizzazione, e nel valutare correttamente il possibile impatto. Non ultimo, la metodologia non riesce a fornire i risultati attesi se non vi è una verifica almeno annuale della validità dei piani, o se questi non vengono aggiornati in parallelo a cambiamenti importanti nelle procedure e processi organizzativi, e se l'organizzazione non si accorge per tempo dei segnali del possibile verificarsi di una determinata minaccia.

Pertanto, la metodologia di business continuity è senz'altro valida per migliorare la resilienza organizzativa, ma non è sufficiente. Perché? Perché, come vedremo in dettaglio più avanti nel testo, ci sono altri fattori che condizionano la corretta gestione dei rischi: primo fra tutti è il personale, dal Vertice ai manager, e ai collaboratori tutti. Ciò senza escludere la complessità e la gravità degli eventi che si manifestano con sempre maggiore frequenza. Questo è un mondo che cambia rapidamente ed esige una risposta adeguata.

Vorrei citare degli autorevoli studiosi ed esperti che condividono questa idea. Ecco un esempio.

> La logica suggerirebbe che aumentando la nostra abilità nel prevedere e assorbire le minacce, i nostri sistemi saranno capaci di sopravvivere meglio in caso di minacce sistemiche.
>
> Mentre sono validi in molte circostanze, essi non rappresentano il cuore di un approccio basato sulla resilienza, e costituiscono una pericolosa assunzione che può lasciare i sistemi in balia dei rischi e sprecare dollari in progetti e sviluppi nella prospettiva di rinforzare i sistemi a fronte di specifiche future minacce. […]
>
> Il mantenere la distinzione fra rischio e resilienza non è soltanto un'esigenza scolastica, ma anche una necessaria policy. Applicare un approccio basato sui rischi a un problema che richiede una soluzione basata sulla resilienza, o viceversa, non fornirà i giusti strumenti per una data attività, e condurrà a investimenti che non producono i necessari cambiamenti richiesti dagli stakeholder (Linkov e Trump, 2019, p. 17).

Condivido queste osservazioni in quanto i rischi non controllabili non possono essere gestiti come quelli prevenibili o strategici: esigono un diver-

so modo di procedere, che vede tra l'altro il forte coinvolgimento di tutto il personale.

Il risk assessment, la business impact analysis, la progettazione dei piani di emergenza, crisis management, recovery, e assorbimento dei danni, sono essenziali, sono condizione necessaria, ma non sufficiente per essere resilienti.

In questo testo si capirà man mano il perché.

Anticipo ai più curiosi che, oltre a evidenziare ed enfatizzare l'importanza del personale, della cultura organizzativa, della leadership e l'impegno del top management (come un esperto aziendale si può attendere), lo standard ISO 22316 afferma: "La progettazione, lo sviluppo e il coordinamento delle discipline di gestione e il loro allineamento con gli obiettivi strategici dell'organizzazione sono fondamentali per migliorare la resilienza organizzativa".

È questa la chiave alla resilienza operativa. Tratteremo più avanti i sistemi di gestione[2].

A questo punto, mi attendo che il lettore si domandi: "Tutto ciò è facile a dirsi… ma come faccio io nella mia organizzazione? Da quali discipline inizio? Come si possono esse integrare?".

Ho già iniziato a esporre le mie idee e più avanti formulerò un'ipotesi di approccio.

Un'ulteriore domanda che può farsi il lettore è: "Vi sono diversi testi di parecchi anni fa che trattano della resilienza e lo stesso standard ISO 22316 è stato pubblicato nel 2017: perché l'argomento è andato scemando, e ora, improvvisamente, si parla diffusamente di resilienza?".

La risposta è facile, in quanto, nel momento in cui sto scrivendo questo testo, tutte le organizzazioni o hanno già iniziato ad apportare dei cambiamenti significativi nella loro operatività, oppure ci stanno riflettendo.

Come vedremo meglio più avanti, c'è stata fino a ora una sottovalutazione dei possibili pericoli e, secondo me, una non totale comprensione dell'importanza dello standard ISO 22316.

È anche vero che i più recenti eventi hanno fatto riflettere le istituzioni e le organizzazioni, private o pubbliche che siano, sulla necessità di un diverso approccio alla protezione dei beni e alla continuità dell'operatività anche a seguito dei recenti eventi disastrosi per estensione e durata. Non dobbiamo però dimenticare che dal 2000 in poi si sono avuti: la crisi economica e quella finanziaria, il terrorismo e la guerra del Golfo, la diffusione della pandemia di aviaria e poi suina, i sempre più frequenti uragani disastrosi nell'ambito dei cambiamenti climatici ecc.

[2] Cfr. il paragrafo "Introduzione ai sistemi di gestione e alle discipline gestionali".

Se degli studiosi e delle aziende specializzate a livello internazionale si sono unite nel definire e pubblicare nel 2017 uno standard sulla resilienza organizzativa, vuol dire che si era manifestata tale esigenza.

Consideriamo quanto segue:

- la globalizzazione: ha facilitato la trasmissione dei virus;
- le minacce naturali: ora sono più frequenti e provocano disastri devastanti;
- gli attacchi informatici: hanno motivazioni diverse (furto, spionaggio, ricatto ecc.), ma l'effetto è drammatico in quanto vi è l'esfiltrazione di dati e informazioni critiche (per es. dati personali, segreti industriali, pratiche commerciali) e soprattutto il blocco dei sistemi per giorni con gravissime conseguenze sul piano finanziario, legale, reputazionale.

Ci sono delle imprese che hanno da diverso tempo predisposto dei piani di emergenza da attuare in caso di un possibile evento disastroso che impatti sulle persone o su processi altamente critici. Citerò, come esempi, le banche, le imprese petrolifere e altre.

Fra queste organizzazioni c'è chi si è concentrata su una determinata causa che colpisce un determinato processo critico. C'è invece chi ha studiato e realizzato dei piani per poter proseguire comunque il servizio, a un livello minimo prefissato e ciò indipendentemente dalla causa.

Se andiamo a vedere un elenco di aziende colpite in modo severo da eventi non previsti possiamo trovare alcune di quelle che hanno molto probabilmente i piani di business continuity, ma che non sono resilienti.

1.2. Le vulnerabilità

In questo paragrafo affronto un problema serio che così sintetizzo: i tecnici della sicurezza, gli informatici e i loro responsabili, se interrogati, sanno dire quali sono le possibili vulnerabilità e come si combattono.

Allora, mi domando, perché i criminali riescono a entrare nei sistemi ICT e rubare dati e informazioni sensibili e riservate? Perché, dopo un attacco hacker riuscito, si scopre che sono state sfruttate delle vulnerabilità? Come mai?

Perché, a mio avviso, come vedremo nel corso di questo manuale, la realtà di tutti i giorni, i problemi non previsti, i cambiamenti di priorità, i budget ristretti che non consentono l'aggiornamento tecnologico, appalti per servizi affidati all'esterno che non sono disegnati e gestiti in modo corretto ecc., fanno sì che la realtà è ben diversa dai progetti e dalla teoria.

Ultimamente è stata brutalmente colpita una grossa organizzazione che è certificata a diversi standard internazionali ed esegue annualmente un checkup sulla privacy. Ciò vuol dire che le certificazioni non servono a nulla? No, ma non bastano. Anzi, potenzialmente potrebbero essere controproducenti, perché creano una falsa sicurezza.

Cosa ci vuole? Un diverso approccio.

E la resilienza è a mio parere la risposta.

Nel box 1.1 riporto i 10 problemi di sicurezza più gravi, redatti da OWASP, un'organizzazione senza scopo di lucro. Per quale motivo lo faccio? Sostanzialmente per due motivi: per la loro rilevanza accertata a livello internazionale (e quindi è bene saperlo), e perché ho potuto verificare che moltissimi attacchi cyber sono riusciti proprio sfruttando anche alcune di queste vulnerabilità.

Mi ricordo ancora che consultai non molti mesi fa un sito web che riportava l'elenco dei siti ove i loro tecnici erano riusciti a mettersi nelle condizioni di poter violare i sistemi di controllo sfruttando debolezze come il Cross Site Scripting XSS e altri (ricordo che se si viola senza autorizzazione un sito, c'è il codice penale che colpisce il malfattore).

Questo problema è noto da anni. Nell'elenco pubblicato sul web c'erano molti dei Comuni italiani che, a gruppi, partecipavano ai miei corsi in AGID.

Mi domando: perché chi si occupa di ICT per un'azienda o un ente pubblico non controlla periodicamente se le nuove applicazioni presentano queste vulnerabilità? Non solo nelle grandi organizzazioni la ricerca delle vulnerabilità viene condotta tramite audit, vulnerability assessment, penetration test ecc., ma se non c'è però la giusta cultura organizzativa e dei rischi, gli attaccanti riusciranno a trovare quel "buco", quel "bug" attraverso il quale entrare.

Non bisogna dimenticare che il problema più serio è rappresentato da milioni di piccole e anche medie realtà che sono esposte a molti più rischi di altre e investono poco in strumenti di prevenzione, e ancora meno in gestione dell'emergenza e continuità del business.

L'economia del Paese è a rischio.

Box 1.1 – OWASP Top 10 application security risks

OWASP Top 10 è un libro/documento di riferimento che delinea i 10 problemi di sicurezza più critici per la sicurezza delle applicazioni web. Il rapporto è redatto da un team di esperti di sicurezza di tutto il mondo. Qui di seguito riporto la classifica del 2017 e ho anche indicato la graduatoria nel 2021. I 10 principali rischi per la sicurezza delle applicazioni web[3]:

[3] https://owasp.org/www-project-top-ten/i, estrazione dei titoli e traduzione a mia cura.