PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 17 - numero 3686 di lunedì 28 dicembre 2015

UNI EN ISO 22313:2014 - Sicurezza della società

Sistemi di gestione per la continuità operativa: Linee guida interpretativa per garantire alla propria azienda un adeguato livello di continuità operativa. Di Adalberto Biasiotti.

Il testo della norma ISO 22313:2012 è stato elaborato dalla commissione tecnica ISO/TC 223 "Societal security" ed è stato recepito come EN ISO 22313:2014 dalla commissione tecnica CEN/TC 391 "Societal and Citizen Security", senza modifiche.

Come si può ben vedere nei riferimenti allegati a questo articolo, in molti altri paesi si è posta la stessa problematica, che è stata affrontata prima a livello internazionale, poi a livello europeo. Un interessante studio per gli esperti del settore consiste proprio nell'analisi comparata delle norme, messe a punto in vari paesi, per estrarre utili spunti che permettano di individuare la miglior soluzione, piuttosto che non la minima.

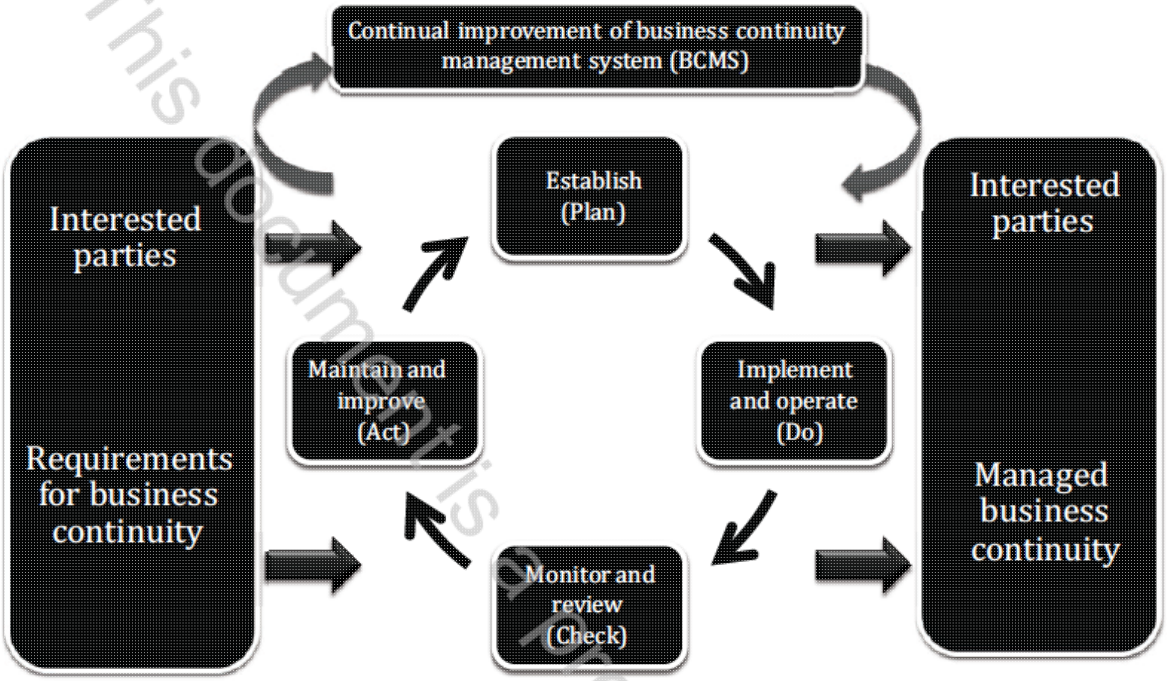
Questa normativa internazionale offre delle linee guida, laddove appropriato, sui requisiti che sono illustrati nella norma EN ISO 22301 ed offre anche raccomandazioni lessicali, assai utili. Ad esempio, quando usa il verbo "dovrebbe" essa fà riferimento ad attività vincolanti, mentre quando usa il verbo "potrebbe" essa fà riferimento ad attività auspicabili.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0397] ?#>

Anche se la intestazione di questa norma assomiglia a quella della norma EN ISO 22301: 2014 ? Societal security ? Business continuity management systems ? Requirements , essa non ripete i requisiti per i sistemi di gestione della continuità operativa, nonché i relativi termini e definizioni.

L'obiettivo di questa norma è invece quello di offrire ulteriori elementi di chiarezza e illustrazione di punti chiave della norma di riferimento, facendo ricorso ad un certo numero di figure.

Tali figure si intendono a fini illustrativi, sono collegate direttamente al testo di questa norma e rappresentano esemplificazioni oltremodo preziose per i professionisti della security, che debbono attuare le indicazioni della norma.



L'importanza della norma sta nel suo cambio di prospettiva, in quanto pone il professionista della security nella condizione di occuparsi in modo allargato della operatività dell'azienda, senza limitarsi solo agli aspetti afferenti a furti, rapine, danneggiamenti ed altro, che rappresentano solo alcuni degli eventi anomali, che possono avere influenza negativa sulla sopravvivenza aziendale.

Un sistema di gestione della continuità operativa sottolinea l'importanza di:
· comprendere le esigenze dell'organizzazione e la necessità di stabilire una politica e degli obiettivi di continuità operativa;
· implementare e attuare controlli e misure, che possono permettere di gestire la capacità dell'azienda di fare fronte a incidenti catastrofici;
· tenere sotto controllo e riesaminare le prestazioni e l'efficacia dei sistemi di BCMS e
· migliorare continuamente questa situazione, sulla base di misure e rilevamenti oggettivi.

Occorre inoltre tener presente che, anche se la norma si applica ad un ente o azienda specifico, essa impone di prestare attenzione anche a possibili riflessi, anche gravi, sulla intera società civile, ove l'ente venisse meno alla sua funzione operativa.. Questa situazione è legata all'attività che viene svolta dall'organizzazione coinvolta.

Si pensi ad esempio ad una situazione di crisi, che impedisca ad una azienda ospedaliera di continuare ad operare al servizio dei cittadini, sul territorio. La situazione di crisi potrebbe essere causata da eventi esterni, come ad esempio un terremoto, oppure una inondazione; in questo caso il professionista della security deve analizzare gli scenari conseguenti e formulare possibili misure di prevenzione, se possibile, o di mitigazione delle conseguenze dell'evento.

Non già l'opportunità, ma addirittura la necessità di condurre uno studio sulla continuità operativa di un'azienda nasce anche dal crescente allarme terrorismo, dai cui attacchi nessun ente od azienda, pubblico o privato, può ritenersi esente.

La guida operativa non si addentra in una analisi dettagliata dei rischi connessi al terrorismo, ma da precedenti studi è possibile ricavare alcuni scenari standardizzati, come ad esempio:

- esplosione di un ordigno sul perimetro dell'insediamento,
- esplosione di un ordigno all'interno dell'insediamento,
- attacco con autobomba lanciata in velocità contro il bersaglio,
- telefonata terroristica,
- invio di una busta esplosiva contenenti agenti tossici.

L'esame di questi eventi è reso particolarmente complesso dal fatto che l'evento in questione può verificarsi in un'area specifica dell'insediamento, in fasce orarie o giorni specifici; appare evidente che le conseguenze dell'esplosione di un ordigno sono ben diverse, a seconda che l'esplosione avvenga nottetempo in una area non occupata dell'azienda, oppure in pieno giorno, lungo la catena di produzione in piena attività.

Il professionista della security deve analizzare tutte queste alternative e elaborare, secondo le linee guida di questa norma, appropriati scenari di messa sotto controllo.

Ma gli scenari presi considerazione non si fermano qui, perché la norma sottolinea che, laddove vi sia un collegamento tra varie aziende od enti, è assai probabile che la incapacità di operare di un'azienda si rifletta anche su tutte le aziende collegate. Occorre quindi esaminare in un'ottica allargata il tema della continuità aziendale.

Anche questa norma utilizza l'ormai famoso schema plan- do- check- act, che ormai è utilizzato sempre più spesso a livello normativo, per la sua chiarezza e facilità di interpretazione (vedi figura).

A proposito della formulazione di questa norma, è bene sottolineare il fatto che la parola "business" viene utilizzata in una interpretazione estremamente allargata, comprendendo qualsiasi attività produttiva o del terziario, che un ente deve sviluppare per raggiungere i propri obiettivi, o per attuare la propria missione.

Per questa ragione essa è applicabile ad organizzazioni grandi, medie e piccole, che operino nel settore industriale, commerciale, dei servizi al pubblico e delle attività non-profit.

È bene tenere presente che l'attività possono essere turbate da una grande varietà di incidenti, alcuni dei quali sono difficili da prevedere o da analizzare. Ecco la ragione per la quale queste linee guida suggeriscono di concentrare l'attenzione sull'impatto conseguente al verificarsi dell'evento, piuttosto che sulla causa; in tal modo è possibile mettere a punto un piano di continuità operativa, che mette in luce le attività dalle quali l'organizzazione dipende per la propria sopravvivenza e permette di mettere a punto un piano che, almeno entro certi limiti, può essere applicabile a vari scenari catastrofici.

È proprio in questo contesto che raccomandiamo caldamente ai lettori di esaminare, in abbinamento a questa norma, anche la norma EN ISO 22317: 2014 ? Societal Security ? Business continuity management systems ? Business impact analysis. Essa offre una linea guida dettagliata per stabilire, realizzare e mantenere un processo di analisi di impatto-BIA -Business Impact Analysis, congruo con i requisiti della norma EN ISO 22301. Come si comprende dalla dizione stessa della norma, una stretta integrazione tra le linee guida sopra illustrate e gli scenari estremi, qui presi in considerazione, consentono di ampliare ed arricchire gli scenari delineati nelle linee guida della norma EN ISO 22313:2014 .

Insieme esaminiamo ora, passo per passo, i temi che vengono presi in esame in questa preziosa guida.
Tanto per cominciare, l'azienda deve evidentemente dotarsi di una linea guida, approvata dall'alta direzione, che deve tracciare i contenuti del programma di gestione della continuità operativa e deve costituire un riferimento non negoziabile per tutti coloro che sono coinvolti nello sviluppo di questo programma.

Una volta definite le linee guida del programma, occorre individuare i soggetti fisici, coinvolti nello sviluppo del programma, con attribuzione di specifiche responsabilità.
In aziende assai complesse ed articolate questo aspetto rappresenta un fattore fondamentale perché, se non vengono definite chiaramente le responsabilità, possono crearsi dei conflitti fra le varie entità aziendali, derivanti da una insufficiente chiarezza degli obiettivi ed anche da possibili rivalità personali.
Non dimentichiamo che ogni uomo (o donna) ha le sue caratteristiche peculiari, che possono favorire o meno i rapporti con altri uomini, pur appartenenti alla stessa azienda ed aventi, almeno si spera, obiettivi comuni.

I passi successivi devono definire i tempi ed i modi di questa pianificazione, analizzando in dettaglio tutti gli scenari ipotizzabili e individuando, per ognuno di essi, le modalità di messa sotto controllo, sia a livello di prevenzione, sia a livello di mitigazione delle conseguenze.
Nelle righe precedenti abbiamo offerto alcuni esempi di scenari, ma la qualità di un piano di gestione della continuità operativa si rileva proprio dalla varietà e articolazione degli scenari ipotizzati, che possono avere origine improvvisa e drammatica, oppure possono essere ricondotti a situazioni che evolvono lentamente, in senso negativo, al passare del tempo.

Il passo successivo consiste nel mettere in pratica quanto è stato definito a livello teorico, mettendo a punto procedure

dettagliate, richiamabili con rapidità e sufficientemente flessibili, da potersi adattare anche a situazioni non perfettamente identificate.

A questo punto occorre vedere se quanto predisposto a tavolino e attuato con appropriate direttive è veramente in grado di fronteggiare gli scenari ipotizzati.
Sulla base di una lunga esperienza, sviluppata in Italia ed in vari paesi del mondo, posso affermare che l'unico strumento affidabile di valutazione della credibilità delle prestazioni di questi piani sta in una simulazione.
Chi scrive, operando nel contesto di protezione dei beni culturali, ha impostato e realizzato simulazioni di emergenze, afferenti ai beni culturali, operando con scenari molto differenziati ed in vari paesi del mondo.

A questo proposito, vale la pena di segnalare ai lettori anche la preziosa norma, che fa riferimento alle modalità con cui è possibile utilizzare volontari in situazioni di emergenza. Nell'esperienza di chi scrive, non è neppure lontanamente concepibile, a fronte di scenari clamorosi, poter impostare gestire un piano di gestione della continuità operativa, che prevede ad esempio il recupero di beni culturali danneggiati, in quantitativi dell'ordine di migliaia di pezzi, senza un contributo determinante da parte di volontari, che devono essere reperiti e selezionati tempestivamente.

La fase finale di ogni simulazione viene chiamata correntemente the briefing e consiste nella analizzare il comportamento di tutti soggetti coinvolti, sulla base delle osservazioni avanzate da soggetti terzi, il cookie unico compito è quello di osservare, senza interferire.

Sistematicamente, nella fase di briefing, vengono messe in evidenza criticità, che sono portate a conoscenza di tutti soggetti coinvolti e che, per solito, portano all'aggiornamento delle procedure precedentemente elaborate.
Secondo lo schema Plan do check act, prima illustrato, le risultanze del the briefing vengono. Utilizzate in un circolo virtuoso, che porta ad un progressivo e costante miglioramento della pianificazione operativa,. Tutte queste attività devono ovviamente essere opportunamente documentate a presente e futura memoria.

La adozione di questo schema offre quindi un'azienda una garanzia non solo teorica, ma convalidata dall'esperienza, errori compresi, che è l'unico strumento che permette di trasformare una garanzia teorica in una ragionevole certezza operativa.

Adalberto Biasiotti
esperto Unesco per la protezione del patrimonio culturale, rappresentante CNCU del Ministero dello sviluppo economico presso tutte le commissioni tecniche normative afferenti alla security

Altri riferimenti normativi
BCM.01-2010 © American Society for Industrial Security and British Standards Institution
AS/NZ 5050 © Standards Australia
SS 540 © Singapore Standards Council
MS 1970 © Malaysian Standards and Accreditation Council

Questo articolo è pubblicato sotto una Licenza Creative Commons.