Standard per la Business Continuity ISO 22301:2019

Indice

Standard per la Business Continuity ISO 22301:2019

- Definizione
- Scopo
- Struttura
- Componenti
- PDCA
- Passi
- Conclusioni

Finalità

- **Lo scopo della business continuity è fare in modo che, in caso di problemi o incidenti, l'azienda o l'ente possa continuare a erogare i propri servizi.**

Standard per la Business Continuity: ISO/IEC 22301

- È uno standard internazionale che fornisce un quadro di riferimento per gestire la capacità di un'organizzazione di continuare ad erogare prodotti e servizi a un livello accettabile, a fronte di eventi avversi che potrebbero verificarsi.
- In particolare, la norma ISO 22301 stabilisce i requisiti per un efficiente Business Continuity Management System (BCMS).

Approfondimenti

1. Evoluzione delle norme
2. Focus
3. Scenario applicativo
4. Definizioni

ISO/IEC 22301: scopo

- La norma specifica i requisiti per pianificare, stabilire, implementare, gestire, monitorare, rivedere, mantenere e migliorare un sistema di gestione per proteggersi dalle interruzioni, ridurre la probabilità di accadimento, prepararsi, rispondere e recuperare nel momento in cui si dovessero presentare.
- I requisiti specificati sono generici e destinati ad essere applicabili a tutte le organizzazioni, o parti di esse, indipendentemente dal tipo, dalle dimensioni e dalla natura dell'organizzazione. La portata dell'applicazione di questi requisiti dipende dall'ambiente operativo e dalla complessità dell'organizzazione.

ISO/IEC 22301: obiettivi

- La ISO è applicabile a tutti i tipi e dimensioni di organizzazioni che:
  - Vogliono implementare, mantenere e migliorare un BCMS
  - Cercano di garantire la conformità con la politica di continuità aziendale dichiarata
  - Necessitano della capacità di continuare ad erogare prodotti e servizi durante un'interruzione ad una capacità predefinita e accettabile
  - Cercano di migliorare la loro resilienza attraverso l'applicazione del BCMS.
- Il documento può essere utilizzato anche per valutare la capacità di un'organizzazione di soddisfare i propri bisogni e gli obblighi di continuità operativa.

ISO/IEC 22301: struttura

Nel documento sono specificati la struttura e i requisiti per l'implementazione e il mantenimento di un efficace sistema di gestione della continuità operativa (BCMS).

- Un'organizzazione deve sviluppare una continuità aziendale che tenga conto della struttura e del tipo di impatto che può accettare in seguito ad un'interruzione. I risultati del mantenimento di un BCMS sono determinati dai requisiti legali, normativi, organizzativi e di settore dell'organizzazione, dai prodotti e dai servizi offerti, dai processi impiegati, dalle dimensioni e dalla struttura dell'organizzazione e, infine, dai requisiti delle parti interessate.

ISO/IEC 22301: struttura

- Un BCMS sottolinea l'importanza di:
  - comprendere le esigenze dell'organizzazione e la necessità di stabilire politiche e obiettivi di continuità aziendale
  - gestire e mantenere processi, capacità e strutture di risposta per garantire che l'organizzazione sopravviva alle interruzioni
  - monitorare e revisionare le prestazioni e l'efficacia del BCMS
  - migliorare di continuo gli obiettivi qualitativi e quantitativi

ISO/IEC 22301: componenti

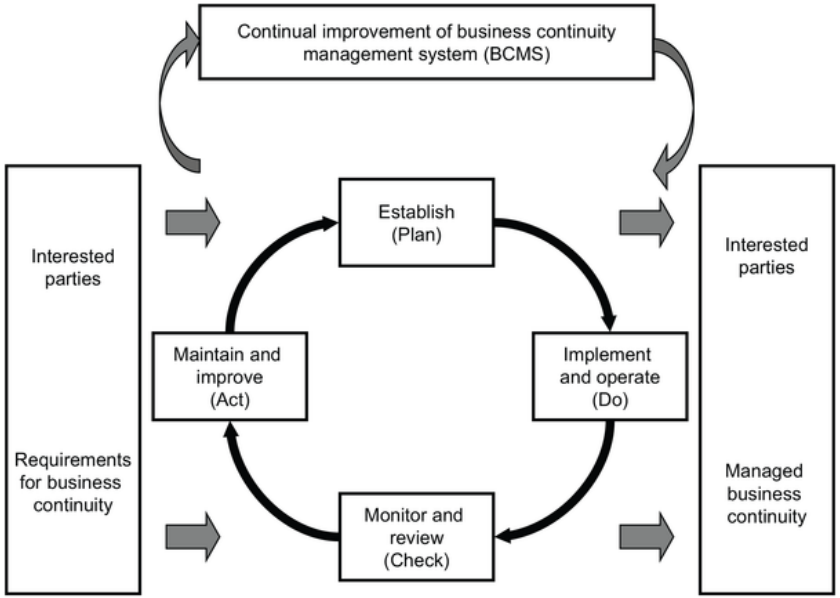
- Un BCMS deve include i seguenti componenti:
  - Una politica di gestione;
  - Le persone competenti con responsabilità definite;
  - I processi gestionali relativi a:
    - Policy;
    - Pianificazione;
    - Implementazione e funzionamento;
    - Valutazione delle prestazioni;
    - Controllo di gestione;
    - Miglioramento continuo;
  - Le informazioni a supporto del controllo operativo che consentano la valutazione delle prestazioni.

ISO/IEC 22301: Plan-Do-Check-Act

Lo standard applica il modello "Plan-Do-Check-Act" (PDCA) alla pianificazione, definizione, attuazione, funzionamento, monitoraggio, revisione, mantenimento e miglioramento continuo dell'efficacia del BCMS di un'organizzazione.

Ciò garantisce un certo grado di coerenza ed integrazione con altri standard dei sistemi di gestione, come la ISO 9001 Sistemi di gestione della qualità, la ISO 14001, Sistemi di gestione ambientale, la ISO / IEC 27001, Sistemi di gestione della sicurezza delle informazioni, la ISO 28000, Specifiche per i sistemi di gestione della sicurezza per la catena di approvvigionamento.

Caveat



Passo 1: Definire il Contesto

I. Comprendere l'organizzazione e il suo contesto

L'organizzazione deve individuare i problemi esterni e interni che sono rilevanti per il suo scopo e che influenzano la sua capacità di raggiungere i risultati previsti dal proprio BCMS.

II. Comprendere i bisogni e le aspettative delle parti interessate

Nel momento in cui l'organizzazione stabilisce il proprio BCMS deve determinare:

a) gli stakeholders rilevanti per il BCMS;
b) i requisiti di queste parti interessate;
c) i requisiti legali e normativi.

III. Determinare l'ambito del sistema di gestione della continuità operativa

L'organizzazione deve determinare i confini e l'applicabilità del BCMS per stabilirne l'ambito.

IV. Sistema di gestione della continuità operativa

L'organizzazione deve stabilire, attuare, mantenere e migliorare continuamente un BCMS, compresi i processi necessari e le loro interazioni, in conformità con i requisiti dello standard.

Passo 2: Compiti della Leadership 1/2

- **Il Top management deve attestare la propria leadership e l'impegno a supportare il BCMS per:**
  - garantire che la politica e gli obiettivi di continuità aziendale siano stabiliti e compatibili con la direzione strategica dell'organizzazione;
  - garantire l'integrazione dei requisiti BCMS nei processi aziendali dell'organizzazione;
  - garantire la disponibilità delle risorse necessarie per il BCMS;
  - comunicare l'importanza di un'efficace continuità aziendale in conformità ai requisiti BCMS;
  - garantire che il BCMS raggiunga i risultati previsti;
  - dirigere e supportare le persone per contribuire all'efficacia del BCMS;
  - supportare gli altri ruoli dirigenziali rilevanti per dimostrare la loro leadership e il loro impegno;
  - promuovere il miglioramento continuo.

Passo 2: Compiti della Leadership 2/2

- **Il Top management deve stabilire una policy di continuità aziendale che:**
  - sia adeguata allo scopo dell'organizzazione;
  - fornisca un quadro per stabilire gli obiettivi di continuità aziendale;
  - includa l'impegno a soddisfare i requisiti applicabili;
  - includa l'impegno per il miglioramento continuo del BCMS.
- **La policy di continuità operativa deve:**
  - essere disponibile sottoforma di informazione documentata;
  - essere comunicata all'interno dell'organizzazione;
  - essere disponibile per gli stakeholders.
- **Il Top management deve assegnare la responsabilità per:**
  - garantire che il BCMS sia conforme ai requisiti dello standard;
  - riferire sull'andamento del BCMS al top management.

Passo 3: Pianificazione 1/3

- **Azioni per affrontare i rischi e le opportunità**

  Nel pianificare il BCMS, l'organizzazione deve considerare le problematiche e i requisiti, di cui al Passo 1: Contesto, e determinare i rischi e le opportunità per:

  a) garantire che il sistema di gestione possa raggiungere i risultati previsti;

  b) prevenire o ridurre gli effetti indesiderati;

  c) ottenere un miglioramento continuo.

  L'organizzazione deve pianificare:

  a) azioni per affrontare tali rischi e opportunità, come:

     1) integrare e attuare le azioni nei suoi processi BCMS,

     2) valutare l'efficacia di queste azioni.

Passo 3: Pianificazione 2/3

- **Obiettivi di continuità aziendale e pianificazione da raggiungere**

Gli obiettivi di continuità operativa devono:

a) essere coerenti con la politica di continuità aziendale;
b) essere misurabili (se possibile);
c) tener conto dei requisiti applicabili;
d) essere monitorati;
e) essere comunicati;
f) essere aggiornati, se del caso.

Nel pianificare come raggiungere gli obiettivi di continuità aziendale, l'organizzazione deve determinare:

a) cosa sarà fatto;
b) quali risorse saranno necessarie;
c) chi sarà responsabile;
d) quando sarà completato;
e) come saranno valutati i risultati.

Passo 3: Pianificazione 3/3

- **Pianificazione delle modifiche al BCMS**

  Quando l'organizzazione valuta la necessità di modificare il BCMS, comprese quelle identificate nella fase di miglioramento, le modifiche devono essere eseguite in modo pianificato.

  L'organizzazione deve considerare:

  a) lo scopo delle modifiche e le loro potenziali conseguenze;

  b) l'integrità del BCMS;

  c) la disponibilità di risorse;

  d) l'attribuzione o la riassegnazione di responsabilità e autorità.

Passo 4: Supporto 1/3

- **Risorse**

  L'organizzazione deve determinare e fornire le risorse necessarie per l'istituzione, l'implementazione, la manutenzione e il miglioramento continuo del BCMS.

- **Competenza**

  L'organizzazione deve:

  a) determinare la competenza necessaria delle persone che svolgono un lavoro che influisce sulle prestazioni della continuità aziendale;

  b) garantire che tali persone siano competenti sulla base di un'adeguata istruzione, formazione o esperienza;

  c) ove applicabile, intraprendere azioni per acquisire le competenze necessarie e valutare l'efficacia delle azioni intraprese;

  d) conservare adeguate le informazioni come prova della competenza.

Passo 4: Supporto 2/3

- **Consapevolezza**

Le persone che svolgono attività, sotto il controllo dell'organizzazione, devono essere consapevoli di:

a) la politica di continuità aziendale;
b) il loro contributo all'efficacia del BCMS, compresi i vantaggi di una migliore performance della continuità operativa;
c) le implicazioni di non conformità ai requisiti BCMS;
d) il proprio ruolo e le proprie responsabilità prima, durante e dopo le interruzioni.

- **Comunicazione**

L'organizzazione deve determinare le modalità di comunicazioni interne ed esterne rilevanti per il BCMS, tra cui:

a) cosa comunicare;
b) quando comunicare;
c) con chi comunicare;
d) come comunicare;
e) chi comunica.

Passo 4: Supporto 3/3

- **Informazioni documentate**

Il BCMS dell'organizzazione deve includere:

a) Le informazioni documentate richieste da questo standard;
b) Le informazioni documentate determinate dall'organizzazione necessarie per l'efficacia del BCMS.

Durante la creazione e l'aggiornamento delle informazioni documentate, l'organizzazione deve garantire:

a) L'identificazione e la descrizione (ad es. titolo, data, autore o numero di riferimento);
b) Il formato (ad es. lingua, versione del software, grafica) e il supporto (ad es. cartaceo, elettronico),
c) La revisione e l'approvazione per l'idoneità e l'adeguatezza.

Le informazioni documentate richieste dal BCMS devono essere controllate per garantire:

a) La disponibilità all'uso, dove e quando è necessario;
b) La protezione (ad es. da perdita di riservatezza, uso improprio o perdita di integrità).

Per il controllo delle informazioni documentate, , a seconda dei casi, si devono affrontare le seguenti attività:

a) La distribuzione, l'accesso, il recupero e l'utilizzo;
b) Il controllo delle modifiche (ad es. controllo della versione);
c) La conservazione e la disponibilità.

Passo 5: Attività operative 1/3

- **Pianificazione e controllo operativi**

  L'organizzazione deve pianificare, attuare e controllare i processi necessari per soddisfare i requisiti e attuare le azioni determinate al passo precedente mediante i seguenti punti:

  a) stabilire i criteri per i processi;
  b) implementare il controllo dei processi secondo i criteri stabiliti;
  c) conservare le informazioni documentate nella misura necessaria per essere certi che i processi siano stati eseguiti come previsto.

  Inoltre, l'organizzazione deve controllare le modifiche pianificate e riesaminare le conseguenze delle modifiche indesiderate, intervenendo, se necessario, per mitigare eventuali effetti avversi.

  Infine, l'organizzazione deve garantire il controllo dei processi esternalizzati e della catena di approvvigionamento.

- **Analisi di impatto sul business e valutazione del rischio**

  L'organizzazione deve implementare e mantenere un processo in grado di analizzare l'impatto sul business e valutare i rischi di interruzione e definire i criteri per la valutazione del potenziale impatto di un'interruzione.

Passo 5: Attività operative 2/3

- **Strategie e soluzioni di continuità operativa**

  L'organizzazione deve identificare e selezionare le strategie di continuità operativa in base ai risultati dell'analisi di impatto sul business e della valutazione del rischio.

  Le strategie di continuità operativa devono comprendere una o più soluzioni.

- **Piani e procedure di continuità operativa**

  L'organizzazione deve implementare e mantenere una struttura per consentire segnalazioni tempestive e comunicazioni alle parti interessate e fornire piani e procedure per gestire l'organizzazione durante un'interruzione.

  I piani e le procedure devono essere utilizzati se necessario per attuare soluzioni di continuità operativa.

Passo 5: Attività operative 3/3

- **Programma di esercitazione**

L'organizzazione deve implementare e mantenere un programma di esercitazione e testing per convalidare nel tempo l'efficacia delle sue strategie e delle soluzioni di continuità aziendale.

L'organizzazione deve condurre esercitazioni e prove che:

a) siano coerenti con i suoi obiettivi di continuità aziendale;
b) si basino su scenari appropriati ben pianificati con scopi e obiettivi chiaramente definiti;
c) sviluppino il lavoro di squadra, la competenza, la fiducia e la conoscenza per coloro che hanno ruoli nel BCMS;
d) riuniscano nel tempo e convalidano tutte le strategie di continuità aziendale;
e) producano relazioni post-esercitazione che contengano i risultati, le raccomandazioni e le azioni per attuare i miglioramenti;
f) siano riviste nel contesto della promozione del miglioramento continuo;
g) vengano eseguiti a intervalli pianificati e quando vi siano cambiamenti significativi all'interno dell'organizzazione o del contesto in cui opera.

L'organizzazione deve agire in base ai risultati dell'esercitazioni e dei test per implementare le modifiche e i miglioramenti necessari.

Passo 6: Valutazione delle performance

- **Monitoraggio, misurazione, analisi e valutazione**

  L'organizzazione deve determinare:

  a) cosa deve essere monitorato e misurato;

  b) i metodi di monitoraggio, misurazione, analisi e valutazione, ove applicabili, per garantire risultati validi;

  c) quando e da chi deve essere effettuato il monitoraggio e la misurazione;

  d) quando e da chi devono essere analizzati e valutati i risultati del monitoraggio e della misurazione.

  Inoltre, deve conservare adeguate informazioni documentate come prova dei risultati.

  Infine, deve valutare le prestazioni e l'efficacia del BCMS.

Passo 7: Miglioramento

- **Non conformità e azioni correttive**

  In caso di non conformità l'organizzazione deve:

  a) reagire alla non conformità e, se è possibile:
     1) agire per controllarla e correggerla;
     2) affrontare le conseguenze.
  b) valutare la necessità di un'azione per eliminare le cause della non conformità affinché non si ripeta o si verifichi altrove:
     1) revisione della non conformità;
     2) determinare le cause della non conformità;
     3) determinare se esistono non conformità simili o potrebbero potenzialmente riverificarsi;
  c) attuare qualsiasi azione necessaria;
  d) rivedere l'efficacia di qualsiasi azione correttiva intrapresa;
  e) se necessario, apportare modifiche al BCMS.

  Le azioni correttive devono essere appropriate agli effetti delle non conformità riscontrate.

  L'organizzazione deve conservare informazioni documentate come prova di:

  a) la causa delle non conformità e le eventuali azioni successive intraprese;
  b) i risultati di qualsiasi azione correttiva.

- **Miglioramento continuo**

  L'organizzazione deve migliorare continuamente l'idoneità, l'adeguatezza o l'efficacia del BCMS. Deve, inoltre, considerare i risultati dell'analisi, della valutazione e i risultati della revisione della direzione, per determinare se ci sono bisogni o opportunità che devono essere affrontati come parte del miglioramento continuo.

Codice dell'Amministrazione Digitale

- **Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i. - Codice dell'amministrazione digitale**
  Art. 50-bis. Continuità operativa.
  1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.
- Il CAD sancisce che gli uffici pubblici devono essere organizzati in modo che sia garantita la digitalizzazione dei servizi. Da tale indicazione consegue, per la Pubblica Amministrazione, anche l'obbligo di assicurare la continuità dei processi che presiedono alla erogazione dei propri servizi, quale presupposto per garantire il corretto e regolare svolgimento della vita nel Paese. Questa affermazione assume particolare significato a fronte del sempre maggiore utilizzo delle tecnologie ICT nella gestione dei dati e dei procedimenti dei singoli enti, che rende necessario adottare tutte le iniziative tese a salvaguardare l'integrità, la disponibilità, la continuità nella fruibilità dei dati.

Conclusioni

- Questa norma favorisce il consolidamento della capacità di organizzare il proprio lavoro per assicurare sostenibilità e continuità. Sarebbe riduttivo vedere la continuità operativa solo come la capacità di continuare a fornire i propri prodotti o servizi in conformità a livelli ritenuti accettabili a seguito di eventi destabilizzanti.
- Per alcune organizzazioni, come quelle che erogano servizi pubblici essenziali, è obbligatorio assicurare l'operatività anche in caso di eventi imprevisti e di incidenti.
- La business continuity non si improvvisa, deve essere pianificata, va tenuta costantemente aggiornata e testata.
- La business continuity coinvolge tutti i soggetti che collaborano con l'organizzazione.
- Senza la business continuity si accetta il rischio di interrompere la propria attività, anche in maniera irreversibile nel caso in cui i danni diventano insostenibili.
- Nella maggior parte dei casi i costi per sostenere la business continuity sono nettamente inferiori all'ammontare dei costi che un'organizzazione deve sostenere per far fronte ai danni causati dalle interruzioni di operatività.

Approfondimento 1: Evoluzione delle norme

- La continuità operativa è la capacità di un'organizzazione di mantenere la fornitura di prodotti e l'erogazione di servizi a livelli accettabili a seguito di un episodio di crisi.
- ISO 22301 è lo standard internazionale per la gestione della continuità operativa.
- È il ruolo più importante che la continuità operativa deve svolgere: proteggere la società e garantire la capacità di reagire agli incidenti, rispondere alle emergenze e alle calamità.
- La norma ISO 22301 è stata creata in risposta al forte interesse per l'originale British Standard BS 25999-2 in sinergia con altre norme locali.
- La versione della ISO 22301:2012 Social Security - Business Continuity Management System - Requirements, è stata pubblicata a maggio 2012 e sostituisce la versione della noma BS 25999-2:2007 - British Standard Part: 2 Specification.
- A Dicembre dello stesso anno 2012 è stata emessa la versione della ISO 22313:2012 Social Security - Business Continuity Management System - Guidance che costituisce la Linea guida.
- A settembre 2016 è stata pubblicata la UNI EN ISO 22301:2014 Sicurezza della società – Sistemi di gestione della continuità operativa - Requisiti.
- Nel novembre 2019 è stato approvato l'aggiornamento.

Approfondimento 2: Focus

- La norma ISO 22301:2019 fornisce i requisiti per un efficiente Business Continuity Management System (BCMS) e si applica a tutte le organizzazioni, siano esse piccole, medie, grandi, locali, nazionali o globali, pubbliche o private.
- Oggigiorno le grandi aziende e i gruppi internazionali, ma anche gli enti della pubblica amministrazione, richiedono – sempre più spesso – ai loro fornitori – di gestire la Business Continuity e dotarsi di un Business Continuity Plan (BCP) e di conseguire certificazioni/attestati che possano maggiormente tutelarli rispetto alla “resilienza” del fornitore, alla capacità di erogazione dei prodotti/servizi anche a fronte di incidenti, eventi catastrofici e altri fenomeni di pari perniciosità.

Approfondimento 3: Scenario applicativo

- Eventi catastrofici naturali, atti di sabotaggio, atti terroristici, turbolenze dei mercati, crisi economiche e geopolitiche, blocco dei sistemi informatici dovuto a malfunzionamenti tecnici o a cyber attack, interruzione dell'alimentazione elettrica, incendi, guerre dei dazi, interruzione della supply chain per fornitori critici ecc., possono interrompere la normale erogazione di prodotti e servizi comportando un fermo operativo, se non addirittura, la chiusura definitiva.
- Le organizzazioni, oggi più che mai, si trovano ad operare in un contesto altamente articolato, globalizzato e digitalizzato e hanno la necessità di proteggersi dalle varie tipologie di eventi che potrebbero provocare un'interruzione delle attività per un certo lasso di tempo, anche breve, con costi diretti e indiretti importanti (i.e. perdite ingenti di fatturato, di quote di mercato, pagamento di sanzioni amministrative – locali o nazionali – o penali contrattuali, danni reputazionali ecc.).
- Pertanto, ogni organizzazione deve dotarsi di strumenti di prevenzione e di risorse, che, oltre a garantire la resilienza organizzativa, dimostrino la capacità di affrontare e di assorbire qualsiasi imprevisto, continuando a conseguire gli obiettivi prefissati.

Approfondimento 4: Definizioni 1/4

Attività: un insieme di una o più attività con un output definito
Revisione: processo sistematico, indipendente e documentato per ottenere elementi di audit e valutarli in modo obiettivo per determinare in che misura i criteri di audit sono soddisfatti
Business continuity: capacità di un'organizzazione di continuare l'erogazione di prodotti e servizi entro tempi accettabili e capacità predefinita relativa a un'interruzione
Sistema di gestione della continuità aziendale BCMS: sistema di gestione per la continuità aziendale
Piano di continuità aziendale: informazioni documentate che guidano un'organizzazione a rispondere ad un'interruzione e riprendere, recuperare e ripristinare l'erogazione di prodotti e servizi coerentemente con i suoi obiettivi di continuità aziendale
Analisi dell'impatto sul business: processo di analisi dell'impatto di un'interruzione sull'organizzazione
Competenza: capacità di applicare conoscenze e abilità per raggiungere i risultati previsti
Conformità: adempimento di un requisito
Conseguenza: risultato di un evento che influisce sugli obiettivi
Miglioramento continuo: attività ricorrente per migliorare le prestazioni
Azione correttiva: azione per eliminare la causa e per prevenire il ripetersi di una non conformità
Guasto: incidente, anticipato o imprevisto, che causa una deviazione non pianificata e negativa dall'erogazione prevista di prodotti e servizi in base agli obiettivi di un'organizzazione
Informazioni documentate: le informazioni devono essere controllate e gestite da un'organizzazione e il supporto su cui sono contenute
Efficacia: la misura in cui vengono realizzate le attività pianificate e i risultati pianificati raggiunti

Approfondimento 4: Definizioni 2/4

Emergenza: evento improvviso, urgente, di solito imprevisto che richiede un'azione immediata
Evento: occorrenza o modifica di un particolare insieme di circostanze
Esercizio: processo per formare, valutare, esercitarsi e migliorare le prestazioni in un'organizzazione
Impatto: esito di una evento che riguarda gli obiettivi
Incidente: evento che può essere o potrebbe provocare un'interruzione, perdita, emergenza o crisi
Informazione: dati elaborati, organizzati e correlati per produrre significato
Parte interessata: persona o organizzazione che può influenzare, essere influenzato o percepire se stesso come influenzato da una decisione o attività
Audizione interna: audit condotto da, o per conto di, un'organizzazione per controllare la gestione e gli altri scopi interni e che può costituire la base per l'autodichiarazione di conformità di un'organizzazione
Probabilità: possibilità che accada qualcosa
Gestione: attività coordinate per dirigere e controllare un'organizzazione
Sistema di gestione: insieme di elementi correlati o interagenti di un'organizzazione per stabilire le politiche, gli obiettivi e i processi per raggiungere tali obiettivi
Misurazione: processo per determinare un valore
Monitoraggio: determinare lo stato di un sistema, un processo o un'attività
Non conformità: inadempimento di un requisito
Oggetto: entità singola e distinta che può essere identificata
Obiettivo: risultato da raggiungere

Approfondimento 4: Definizioni 3/4

Organizzazione: ente o gruppo di persone che hanno la responsabilità, l'autorità e le relazioni per raggiungere i suoi obiettivi
Esternalizzare: fare un accordo in cui un'organizzazione esterna svolge parte della funzione o del processo di un'organizzazione
Prestazione: risultato misurabile
Valutazione delle prestazioni: processo per determinare i risultati misurabili in base ai criteri impostati
Personale: persone che lavorano per e sotto il controllo dell'organizzazione
Pianificazione: parte del management focalizzata sulla definizione degli obiettivi di continuità aziendale e sulla specifica dei processi operativi necessari e delle risorse correlate al raggiungimento degli obiettivi di continuità aziendale
Politica: obiettivi e direzione di un'organizzazione espresse formalmente dal suo top management
Attività prioritaria: attività a cui viene data urgenza al fine di evitare impatti inaccettabili per l'impresa durante un'interruzione
Procedura: modo specifico per svolgere un'attività o un processo
Processi: insieme di attività correlate o interagenti che trasforma gli input in output
Prodotto o servizio: output o risultati forniti da un'organizzazione alle parti interessate
Protezione: misure che salvaguardano e consentono a un'organizzazione di prevenire o ridurre l'impatto di una potenziale minaccia
Registrazione: documentare i risultati ottenuti o fornire prove delle attività svolte
Recupero: ripristino e miglioramento, se del caso, di operazioni, strutture, mezzi di sussistenza o condizioni di vita delle organizzazioni, compresi gli sforzi per ridurre i fattori di rischio
Requisiti: necessità o aspettativa dichiarata, generalmente implicita o obbligatoria
Resilienza: capacità di assorbire e adattarsi in un ambiente che cambia

Approfondimento 4: Definizioni 4/4

Revisione: attività intrapresa per determinare l'idoneità, l'adeguatezza e l'efficacia del sistema di gestione e dei suoi elementi componenti per raggiungere gli obiettivi stabiliti
Rischio: effetto dell'incertezza sugli obiettivi
Valutazione del rischio: processo generale di identificazione, analisi e valutazione del rischio
Gestione del rischio: attività coordinate per dirigere e controllare un'organizzazione in relazione al rischio
Catena di fornitura: relazione bidirezionale tra organizzazioni, persone, processi, logistica, informazione, tecnologia e risorse impegnate in attività e creazione di valore dall'approvvigionamento di materiali attraverso la consegna di prodotti e servizi
Test: tipo unico e particolare di esercizio che incorpora l'aspettativa di un elemento pass o fail all'interno dello scopo o degli obiettivi dell'esercizio in programma
Alta direzione: persona o gruppo di persone che dirige e controlla un'organizzazione ai massimi livelli
Formazione: attività progettate per facilitare l'apprendimento e lo sviluppo di conoscenze, abilità e capacità e per migliorare le prestazioni di compiti o ruoli specifici
Verifica: la conferma, attraverso la fornitura di prove, che sono stati soddisfatti i requisiti specificati
Ambiente di lavoro: insieme di condizioni in cui viene eseguito il lavoro

Approfondimento Passo 5: Attività operative

Approfondimento

- Business impact analysis / Analisi di impatto sul business
- Risk assessment / Valutazione del rischio
- Individuazione e selezione delle strategie e soluzioni
- Requisiti delle risorse
- Implementazione delle soluzioni
- Struttura di risposta
- Avvisi e comunicazione
- Piani di continuità aziendale
- Recupero

Approfondimento 5:
Analisi di impatto sul business

L'organizzazione deve attuare e mantenere un processo per determinare le priorità e i requisiti di continuità operativa che sia in grado di:

a) definire le categorie di impatto e i criteri rilevanti per il contesto dell'organizzazione;

b) utilizzare queste categorie e i criteri per misurare l'impatto;

c) identificare le attività a supporto della fornitura di prodotti e servizi;

d) analizzare gli impatti nel tempo derivanti dall'interruzione di tali attività;

e) identificare il tempo entro il quale gli impatti della mancata ripresa delle attività diventano inaccettabili per l'organizzazione;

f) stabilire i termini prioritari entro il tempo identificato per riprendere le attività interrotte ad una capacità minima accettabile specificata;

g) utilizzare gli impatti aziendali per identificare le attività prioritarie;

h) determinare quali risorse sono necessarie per supportare le attività prioritarie;

i) determinare le dipendenze e le interdipendenze delle attività prioritarie.

Approfondimento 6: Valutazione del rischio

L'organizzazione deve attuare e mantenere un processo sistematico di valutazione del rischio.

Questo processo può essere eseguito in conformità alla ISO 31000.

L'organizzazione deve:

a) identificare i rischi di interruzione delle attività prioritarie dell'organizzazione e delle loro risorse di supporto;

b) analizzare sistematicamente i rischi di interruzione;

c) valutare i rischi di interruzione che richiedono un trattamento.

Approfondimento 7:
Individuazione e selezione delle strategie e soluzioni

L'organizzazione deve identificare e selezionare le strategie e le soluzioni di continuità aziendale appropriate tenendo conto dei costi associati per:

a) rispondere alle interruzioni;

b) continuare e recuperare le attività prioritarie e le risorse necessarie per soddisfare la consegna di prodotti e servizi alla capacità concordata nel tempo.

Per le attività prioritarie, l'organizzazione deve identificare e selezionare le strategie e le soluzioni tenendo conto degli obiettivi di continuità aziendale, del costo e del tipo di rischio che l'organizzazione può assumersi per:

a) ridurre la probabilità di interruzione;

b) abbreviare il periodo di interruzione;

c) limitare l'impatto dell'evento sui prodotti e servizi dell'organizzazione.

Approfondimento 8: Requisiti delle risorse

L'organizzazione deve determinare i requisiti delle risorse per implementare le soluzioni di continuità aziendale selezionate.

I tipi di risorse devono includere, ma non essere limitati, a:

a) personale;
b) informazioni e dati;
c) infrastrutture fisiche come edifici, luoghi di lavoro o altre strutture e servizi connessi;
d) attrezzature e materiali di consumo;
e) tecnologie dell'informazione e della comunicazione (TIC);
f) trasporto;
g) finanza;
h) partner e fornitori.

Approfondimento 9: Implementazione delle soluzioni

L'organizzazione deve implementare soluzioni di continuità aziendale selezionate in modo che possano essere attivate quando necessario.

Approfondimento 10: Struttura di risposta

L'organizzazione deve implementare e mantenere una struttura che identifica una o più squadre responsabili della risposta alle interruzioni.

I ruoli e le responsabilità di ciascuna squadra e i rapporti tra le squadre devono essere chiaramente indicati.

Le squadre devono essere preparate a:

a) valutare la natura e l'entità di un'interruzione e il suo impatto potenziale;
b) valutare l'impatto rispetto a soglie predefinite che giustifichino l'avvio di una risposta formale;
c) attivare una risposta di continuità aziendale adeguata;
d) pianificare le azioni che devono essere intraprese;
e) stabilire le priorità (partendo dalla sicurezza delle persone come prima priorità);
f) monitorare gli effetti dell'interruzione e la risposta dell'organizzazione;
g) attivare le soluzioni di continuità aziendale;
h) comunicare con le parti interessate, le autorità e i media interessati.

Per ogni squadra sarà:

a) identificato il personale con la responsabilità, l'autorità e la competenza necessarie per svolgere il ruolo designato;
b) documentata la procedura utilizzata per l'attivazione, il funzionamento, il coordinamento e la comunicazione della risposta.

Approfondimento 11:
Avvisi e comunicazione

L'organizzazione deve documentare e mantenere le procedure per:

a) comunicare internamente ed esternamente alle parti interessate, incluso cosa, quando, con chi e come comunicare;
b) ricevere, documentare e rispondere alle comunicazioni delle parti interessate, incluso qualsiasi sistema di consulenza sui rischi nazionale o regionale o equivalente;
c) garantire la disponibilità dei mezzi di comunicazione durante un'interruzione;
d) facilitare la comunicazione strutturata con i responder;
e) i dettagli della risposta ai media dell'organizzazione a seguito di un incidente, inclusa una strategia di comunicazione;
f) registrare i dettagli dell'interruzione, le azioni intraprese e le decisioni prese.

Laddove applicabile, devono anche essere considerati e implementati:

a) Gli avvisi alle parti potenzialmente colpite da un'interruzione effettiva o imminente;
b) Un adeguato coordinamento e comunicazione tra le organizzazioni con più risposte;

Le procedure di comunicazione e allertamento devono essere esercitate come parte del programma di esercitazione.

Approfondimento 12:
Piani di continuità aziendale

I piani di continuità operativa devono fornire indicazioni e informazioni che aiutino i team a rispondere ad un'interruzione ed assistere l'organizzazione per riprendersi dopo un'interruzione.

I piani di continuità operativa devono contenere:

a) i dettagli delle azioni che i team intraprenderanno per continuare o recuperare le attività prioritarie entro tempi prestabiliti e per monitorare gli effetti dell'interruzione e la risposta dell'organizzazione;
b) il riferimento alla soglia e al processo predefinito per l'attivazione della risposta;
c) le procedure per consentire la consegna dei prodotti e dei servizi alle capacità concordate alle parti interessate;
d) i dettagli per gestire le conseguenze immediate di un'interruzione tenendo in debita considerazione:
    1) il benessere delle persone;
    2) la prevenzione di ulteriori perdite o indisponibilità di attività prioritarie;
    3) la protezione dell'ambiente;
e) un processo per fermarsi una volta che l'incidente è finito.

Ogni piano deve includere:

a) Lo scopo e l'ambito di applicazione e degli obiettivi;
b) I ruoli, le responsabilità del team che implementerà il piano;
c) Le azioni e le risorse per implementare le soluzioni;
d) le informazioni di supporto necessarie per attivare (compresi i criteri di attivazione), operare, coordinare e comunicare le azioni del team;
e) Le interdipendenze interne ed esterne;
f) Il fabbisogno di risorse;
g) Gli obblighi di segnalazione.

Ogni piano deve essere utilizzabile e disponibile nel momento e nel luogo in cui è richiesto.

Approfondimento 13: Recupero

L'organizzazione deve disporre di processi documentati per ripristinare e riavviare le attività di business dalle misure temporanee adottate per supportare i normali requisiti aziendali durante e dopo un'interruzione.

Approfondimento Passo 6: Valutazione delle performance

Approfondimento

- Valutazione dei piani, delle procedure e della capacità di continuità operativa
- Audit interno
- Controllo di gestione

Approfondimento 14:
Valutazione dei piani, delle procedure e della capacità di continuità operativa

L'organizzazione deve valutare l'idoneità, l'adeguatezza e l'efficacia dei propri piani, delle procedure e della capacità di continuità operativa.

Tali valutazioni devono essere eseguite mediante revisioni periodiche, analisi, esercitazioni, prove, relazioni post-incidente e valutazioni delle prestazioni.

L'organizzazione deve valutare periodicamente la conformità ai requisiti legali e regolamentari, alle migliori pratiche del settore, alla propria politica e agli obiettivi di continuità aziendale.

L'organizzazione deve effettuare le valutazioni ad intervalli pianificati dopo un incidente o un'attivazione e quando si verificano cambiamenti significativi devono essere aggiornate in modo tempestivo.

Approfondimento 15: Audit interno

L'organizzazione deve condurre audit interni a intervalli pianificati per fornire informazioni sul fatto che il BCMS:

a) è conforme a:
   1) i requisiti dell'organizzazione per il suo BCMS,
   2) i requisiti del presente documento;
b) è implementato e mantenuto efficacemente.

L'organizzazione deve:

a) pianificare, stabilire, attuare e mantenere un programma di audit, compresi la frequenza, i metodi, le responsabilità, i requisiti di pianificazione e le relazioni. I programmi di audit tengono conto dell'importanza dei processi interessati e dei risultati di audit precedenti;
b) definire i criteri di audit e la portata di ciascun audit;
c) selezionare i revisori e condurre audit per garantire l'obiettività e l'imparzialità del processo di audit;
d) assicurare che i risultati degli audit siano comunicati alla direzione competente;
e) conservare le informazioni documentate come prove dell'attuazione del programma e dei risultati dell'audit.

Approfondimento 16: Controllo di gestione 1/2

Il Top management deve verificare il BCMS, a intervalli pianificati, per garantirne l' idoneità, l'adeguatezza e l'efficacia.

Il riesame della direzione deve comprendere:

a) lo stato delle azioni delle precedenti revisioni;
b) i cambiamenti nelle questioni esterne e interne che sono rilevanti per il BCMS;
c) le informazioni sull'andamento della continuità operativa;
d) i feedback delle parti interessate;
e) la necessità di modifiche al BCMS, compresi le politica e gli obiettivi;
f) le procedure e le risorse che potrebbero essere utilizzate nell'organizzazione per migliorare le prestazioni e l'efficacia del BCMS;
g) le informazioni fornite dalla BIA e la valutazione del rischio;
h) i rischi o i problemi non adeguatamente affrontati in una precedente valutazione del rischio;
i) i risultati di esercitazioni e prove;
j) le lezioni apprese e le azioni derivanti da mancati incidenti e interruzioni;
k) l'opportunità di miglioramento continuo.

Approfondimento 16: Controllo di gestione 2/2

I risultati del riesame della direzione comprendono le decisioni relative all'opportunità di effettuare un miglioramento continuo e l'eventuale necessità di apportare modifiche al BCMS per migliorarne l'efficienza e l'efficacia e includere quanto segue:

a) variazioni del campo di applicazione del BCMS;

b) aggiornamento dell'analisi dell'impatto aziendale, della valutazione del rischio, delle strategie e delle soluzioni di continuità aziendale e dei piani di continuità operativa;

c) modifica delle procedure e dei controlli per rispondere ai problemi interni o esterni che possono avere un impatto sul BCMS;

d) come sarà misurata l'efficacia dei controlli.

L'organizzazione deve conservare informazioni come prova dei risultati delle revisioni della direzione e:

a) comunicare i risultati del riesame della direzione alle parti interessate pertinenti;

b) intraprendere le azioni appropriate relative a tali risultati.