L'Accademia su misura per i professionisti HSE

Dispensa formativa

Ruoli, impatti e decisioni: architettura della continuità operativa

Sommario

1. Introduzione alla business continuity

La continuità operativa è la capacità di un'organizzazione di garantire le proprie attività essenziali anche in presenza di eventi critici o imprevisti. Questa disciplina si colloca all'interno della più ampia cornice della resilienza organizzativa e rappresenta una leva fondamentale per proteggere persone, asset e servizi, assicurando al contempo la fiducia degli stakeholder.

Definizione e finalità della continuità operativa

La business continuity si riferisce all'insieme di misure, procedure e strategie volte a mantenere o ripristinare il funzionamento delle attività critiche durante e dopo eventi dirompenti. L'obiettivo non è solo evitare il blocco delle operazioni, ma assicurare la coerenza con la missione dell'organizzazione anche in condizioni straordinarie.

Queste misure includono la pianificazione, l'assegnazione di responsabilità, l'adozione di strumenti di risposta rapida e il continuo aggiornamento dei piani sulla base delle esperienze acquisite e dei cambiamenti nel contesto.

Relazione tra continuità e resilienza organizzativa

La continuità è una componente operativa della resilienza. Se la resilienza rappresenta la capacità complessiva di adattarsi, assorbire gli shock e imparare da essi, la business continuity fornisce l'infrastruttura di processo necessaria per reagire in modo efficace a un evento critico. In questo senso, si tratta di uno strumento concreto che consente all'organizzazione di non interrompere il proprio ciclo vitale anche sotto pressione.

Eventi critici: issue, incidenti e crisi

Non tutti gli eventi hanno lo stesso impatto. La capacità di differenziare correttamente la natura dell'evento è essenziale per adottare la risposta adeguata:

- **Issue:** evento minore, contenuto, risolvibile con risorse ordinarie.
- **Incidente:** evento con impatto significativo ma gestibile a livello locale.
- **Crisi:** evento straordinario che minaccia la continuità, richiede decisioni rapide, coinvolge più livelli dell'organizzazione e può compromettere la reputazione.

Questa classificazione è utile per definire le soglie di attivazione del piano di continuità e individuare con chiarezza ruoli, escalation e modalità operative.

Perché è importante garantirla: impatto, aspettative sociali, reputazione

In molti settori – pubblici, strategici, scientifici – l'interruzione delle attività non comporta solo perdite economiche, ma anche ripercussioni sociali e danni reputazionali. I cittadini,

gli utenti e gli stakeholder si aspettano che i servizi essenziali siano garantiti anche in condizioni critiche, e questa aspettativa rappresenta un obbligo implicito per le organizzazioni.

Garantire la continuità operativa significa anche tutelare la reputazione e la credibilità dell'ente, consolidando nel tempo la fiducia interna ed esterna. In questa prospettiva, la business continuity non è solo una misura tecnica, ma una responsabilità organizzativa e culturale.

2. Ruoli e responsabilità nella gestione delle emergenze

Una gestione efficace della continuità operativa richiede chiarezza nei ruoli e un coordinamento strutturato tra le diverse figure coinvolte. In particolare, è essenziale comprendere la distinzione tra funzioni operative e tecnico-preventive, e valorizzare la collaborazione tra chi prende decisioni sul campo e chi garantisce coerenza con le misure di sicurezza.

Incident Coordinator: compiti, funzioni, modello INFN

L'Incident Coordinator è la figura che assume il comando operativo in caso di evento critico. Nominato formalmente dal vertice organizzativo, ha il compito di attivare le procedure, prendere decisioni rapide e interfacciarsi con il livello superiore (es. Comitato di crisi).

Nel modello INFN, il suo ruolo è ben definito: opera localmente, è presente fisicamente sul campo, mantiene la tracciabilità degli eventi e supporta la direzione nella gestione delle emergenze. È una figura di snodo tra il livello operativo e quello decisionale, e garantisce che la risposta sia tempestiva, coordinata e documentata.

RSPP: ruolo tecnico-preventivo e supporto alla sicurezza

Il Responsabile del Servizio Prevenzione e Protezione (RSPP) è una figura normata, incaricata di tutelare la salute e la sicurezza dei lavoratori. Le sue competenze includono la valutazione dei rischi, la proposta di misure preventive, la formazione e il monitoraggio continuo.

Durante un'emergenza, il suo ruolo non è quello di comando: agisce come supporto tecnico, valutando le implicazioni delle decisioni prese, verificando la conformità alle norme di sicurezza e proponendo eventuali modifiche o alternative più sicure.

Confronto tra funzioni operative e consulenziali

L'Incident Coordinator e l'RSPP rappresentano due approcci complementari alla gestione delle emergenze:

- L'Incident Coordinator ha una funzione **esecutiva e operativa**: prende decisioni sul momento, attiva risorse, guida l'azione.
- L'RSPP svolge una funzione **tecnica e preventiva**: analizza le situazioni, valuta i rischi, assicura la coerenza con i sistemi di gestione e le normative.

Questa distinzione consente di evitare conflitti di competenza e di garantire una risposta completa: tempestiva ma anche sicura.

Team locale: composizione e integrazione dei ruoli

Nel modello operativo INFN, la gestione delle emergenze è affidata a un **Incident Management Team locale**, presieduto dal Direttore della struttura. Ne fanno parte:

- l'Incident Coordinator,
- l'RSPP,
- i responsabili tecnici delle aree o degli impianti coinvolti,
- un referente per la comunicazione.

Questo assetto consente di unire capacità decisionali, competenze operative, visione tecnica e gestione della comunicazione. La presenza di un team multidisciplinare garantisce che le scelte siano condivise, realistiche e attuabili.

La chiarezza nella definizione dei ruoli e la collaborazione tra figure diverse sono premesse indispensabili per un sistema di continuità operativa realmente funzionante.

3. Norme di riferimento

Un sistema di business continuity efficace si fonda su principi culturali e strumenti operativi riconosciuti a livello internazionale. Le due norme principali che guidano l'impostazione moderna della continuità operativa sono la **ISO 22316**, dedicata alla resilienza organizzativa, e la **ISO 22301**, che definisce i requisiti per un sistema di gestione documentato (BCMS – Business Continuity Management System).

ISO 22316: principi della resilienza organizzativa

La ISO 22316 non è una norma prescrittiva, ma culturale. Offre una visione sistemica della resilienza come **capacità di un'organizzazione di adattarsi, assorbire uno shock e continuare a operare** in condizioni complesse.

Tra i principi fondamentali:

- **Flessibilità**: capacità di adattare processi e risorse in base al contesto.
- **Consapevolezza situazionale**: lettura tempestiva dei segnali di rischio.
- **Comunicazione efficace**: scambio di informazioni chiaro, tempestivo e bidirezionale.
- **Leadership diffusa**: possibilità di prendere decisioni anche in assenza del vertice.
- **Apprendimento continuo**: capacità di trarre insegnamenti da ogni evento critico.

La resilienza, secondo questa norma, è un'attitudine che va coltivata attraverso la cultura interna e il coinvolgimento di tutti i livelli dell'organizzazione.

ISO 22301: struttura del Business Continuity Management System (BCMS)

La ISO 22301 è una norma gestionale: definisce i requisiti minimi per realizzare un sistema strutturato di business continuity. È applicabile a qualsiasi organizzazione e si basa sul ciclo **PDCA (Plan – Do – Check – Act)**.

Le sette sezioni chiave della norma sono:

- **Contesto dell'organizzazione**: analisi dei fattori esterni e interni, e delle parti interessate.
- **Leadership**: impegno della direzione, ruoli, responsabilità, politica di continuità.
- **Pianificazione**: identificazione degli obiettivi e dei rischi connessi.
- **Supporto**: risorse, competenze, documentazione, comunicazione interna ed esterna.
- **Operatività**: identificazione delle attività critiche e definizione delle misure di risposta.
- **Valutazione delle prestazioni**: audit, monitoraggio, analisi dei risultati.
- **Miglioramento continuo**: azioni correttive, aggiornamenti, revisione del sistema.

Questo approccio consente di costruire un sistema coerente, verificabile e in grado di evolvere nel tempo.

Connessione tra cultura e metodo

Le due norme non si contraddicono, ma si completano. La **ISO 22316** fornisce il quadro culturale e comportamentale; la **ISO 22301** propone la struttura tecnica e gestionale.

Per rendere davvero efficace un piano di continuità operativa è necessario che cultura e metodo viaggino insieme: **non basta avere un sistema documentato se non esiste la cultura della prontezza**, così come non basta la cultura se mancano ruoli, strumenti e procedure.

L'integrazione tra questi due livelli è il cuore della continuità operativa moderna.

4. Business Impact Analysis (BIA)

La Business Impact Analysis (BIA) è uno degli strumenti centrali della business continuity. Permette di identificare le attività critiche di un'organizzazione e di valutarne la vulnerabilità rispetto a possibili interruzioni. È il momento in cui la teoria incontra la realtà operativa: da questa analisi dipendono le priorità, le risorse e le strategie che verranno adottate.

Finalità e logica della BIA

La BIA non serve solo a raccogliere informazioni: è uno strumento decisionale. L'obiettivo è determinare:

- quali attività non possono essere interrotte senza danni rilevanti;
- quali sono le conseguenze potenziali di un'interruzione prolungata;
- quanto tempo è possibile resistere prima che l'impatto diventi inaccettabile;
- quali risorse sono essenziali per evitare o ridurre i danni.

La BIA consente di collegare ogni attività a un impatto misurabile e quindi di definire un ordine di priorità tra i processi aziendali.

Parametri chiave: MTPD, RTO, RPO

La ISO 22301 identifica tre parametri fondamentali per la BIA:

- **MTPD (Maximum Tolerable Period of Disruption):** è il tempo massimo entro cui un'attività deve essere ripristinata per evitare danni irreversibili o inaccettabili. Superato questo limite, l'impatto diventa insostenibile.
- **RTO (Recovery Time Objective):** è il tempo che ci si pone come obiettivo per il ripristino dell'attività, all'interno del margine consentito dal MTPD.

- **RPO (Recovery Point Objective):** rappresenta la perdita di dati o produzione considerata accettabile. È un parametro tipico per i sistemi informatici, ma può essere applicato anche ad altri contesti.

Questi tre valori aiutano a tradurre in termini operativi il livello di tolleranza dell'organizzazione all'interruzione.

Tipologie di conseguenze da valutare

Una BIA efficace tiene conto di diverse categorie di impatto:

- **Operativo:** perdita di funzionalità, blocco di processi, impossibilità di erogare servizi.
- **Finanziario:** costi diretti, penali contrattuali, mancati ricavi.
- **Reputazionale:** perdita di fiducia da parte di stakeholder, clienti, partner istituzionali.
- **Legale e regolatorio:** violazione di obblighi, interruzione di adempimenti normativi, sanzioni.

Valutare le conseguenze secondo più prospettive consente di costruire un'analisi completa e di giustificare meglio le scelte strategiche.

Relazione tra BIA e strategie operative

La BIA non è un documento fine a sé stesso: deve fornire la base per tutte le strategie di risposta. Se i parametri MTPD, RTO e RPO vengono stabiliti senza un'analisi solida, il piano rischia di risultare irrealistico o inefficace.

Le misure operative – come ridondanza, delocalizzazione, smart working – devono essere progettate in funzione delle criticità individuate. Ogni azione deve avere una ragione precisa, fondata sull'impatto atteso.

Connessione con il risk assessment

La BIA valuta le conseguenze di un'interruzione; il **risk assessment** ne analizza le cause. I due strumenti sono distinti ma complementari:

- la BIA si concentra sul "**cosa succede se**";
- il risk assessment si chiede "**perché potrebbe succedere**".

L'RSPP gioca un ruolo fondamentale nel risk assessment, individuando i pericoli e proponendo misure preventive. Una buona integrazione tra analisi dell'impatto e

valutazione del rischio consente di **prevenire gli scenari peggiori**, non solo di reagire ad essi.

5. Strategie di risposta

Una volta individuate le attività critiche e valutato l'impatto potenziale di un'interruzione, è necessario definire come garantire la continuità. Le strategie di risposta traducono l'analisi in azione: rappresentano le soluzioni pratiche che permettono all'organizzazione di resistere, adattarsi e ripartire. La loro efficacia dipende da tre fattori: **tempestività, sostenibilità e coerenza con i rischi valutati**.

Ridondanza, delocalizzazione, smart working

Le strategie più comuni includono:

- **Ridondanza:** duplicazione di sistemi, impianti o risorse. Ad esempio, un generatore di backup o un server secondario. È utile per attività ad alta criticità, ma può essere costosa.
- **Delocalizzazione temporanea:** trasferire l'attività in altra sede già predisposta. Questa strategia richiede pianificazione anticipata e accordi logistici chiari.
- **Smart working:** soluzione adatta per le attività amministrative o di supporto. Può essere attivato rapidamente se già previsto nel piano di continuità.

La scelta tra queste opzioni dipende dalla natura dell'attività, dal contesto e dalle risorse disponibili.

Appalti di emergenza e forniture alternative

In molti casi, la continuità dipende da soggetti esterni. Per garantire la disponibilità di beni o servizi anche in condizioni critiche, è possibile:

- **Prevedere appalti di emergenza:** contratti attivabili rapidamente con fornitori già selezionati.
- **Pianificare forniture alternative:** identificare fonti secondarie affidabili per materiali o componenti chiave.

Queste misure richiedono una **valutazione preventiva della filiera** e una formalizzazione contrattuale compatibile con lo scenario emergenziale.

Equilibrio tra tempestività e sicurezza

Agire rapidamente non significa agire in modo improvvisato. Ogni strategia deve trovare un equilibrio tra urgenza ed efficacia:

- **L'Incident Coordinator** prende decisioni rapide per evitare escalation e garantire la continuità.
- **L'RSPP** verifica che le scelte siano conformi alle misure di sicurezza, segnalando eventuali rischi aggiuntivi.

Un'azione è efficace solo se tiene insieme **rapidità operativa e prudenza tecnica**. La collaborazione tra questi due ruoli è fondamentale per evitare decisioni affrettate, incoerenti o potenzialmente dannose.

Dialogo tra Incident Coordinator e RSPP

Le strategie operative non si definiscono in isolamento. Devono essere **condivise e validate** da chi conosce sia il contesto operativo che i vincoli di sicurezza.

Il dialogo tra Incident Coordinator e RSPP permette di:

- integrare i punti di vista;
- prevenire conflitti o sovrapposizioni;
- migliorare la qualità delle decisioni;
- adattare la risposta al contesto specifico.

La strategia nasce da questo confronto: ciò che si può fare, e ciò che si deve fare, devono incontrarsi in una scelta coerente.

6. Il piano di continuità operativa

Il piano di continuità operativa è il documento che raccoglie e formalizza tutte le informazioni, i ruoli, le strategie e le procedure necessarie per affrontare un'interruzione. Non è un documento teorico: deve essere **chiaro, utilizzabile e aggiornato**. È uno strumento di coordinamento che permette all'organizzazione di agire con efficacia in condizioni critiche.

Obiettivi del piano: ripristino, coordinamento, chiarezza

Il piano ha tre obiettivi fondamentali:

- **Rispondere con prontezza:** attivare immediatamente le misure necessarie per contenere l'impatto e garantire la sicurezza.
- **Ripristinare le attività critiche:** riportare il funzionamento entro i tempi compatibili con gli obiettivi RTO e MTPD.
- **Coordinare strutture e responsabilità:** evitare ambiguità su chi decide, chi esegue, chi comunica.

Un piano ben costruito evita improvvisazioni e consente una gestione ordinata anche nelle prime fasi di un evento inatteso.

Struttura secondo ISO 22301: contenuti essenziali

La ISO 22301 definisce una struttura chiara, che può essere adattata in base alle dimensioni e alla complessità dell'organizzazione. Gli elementi fondamentali sono:

- **Identificazione delle attività critiche:** basata sulla BIA, con priorità e vincoli ben definiti.
- **Parametri MTPD, RTO e RPO:** indicano i limiti temporali e supportano la pianificazione delle risposte.
- **Strategia di continuità:** descrizione delle misure da attivare in caso di interruzione (es. ridondanza, smart working, trasferimento).
- **Ruoli e responsabilità:** elencazione chiara dei soggetti coinvolti, con relative mansioni, modalità di attivazione e sostituzione.
- **Procedure operative:** sequenza delle azioni da compiere in risposta all'evento, con istruzioni pratiche e contatti.
- **Piano di comunicazione:** modalità per informare tempestivamente le persone coinvolte, i referenti esterni, la direzione.
- **Meccanismi di monitoraggio e revisione:** verifica periodica del piano, aggiornamenti dopo eventi reali o simulati.

Questa struttura consente di costruire un documento accessibile, coerente e funzionale.

Integrazione dei ruoli nel piano

Il piano di continuità non può prescindere dalla presenza e collaborazione dei ruoli chiave:

- **Incident Coordinator:** attiva il piano, coordina le azioni, mantiene la tracciabilità delle decisioni.
- **RSPP:** verifica la coerenza tecnica delle azioni, valuta i rischi secondari, supporta l'aggiornamento delle misure.
- **Direzione:** assegna risorse, garantisce l'allineamento con la strategia organizzativa, approva le revisioni.

L'efficacia del piano dipende dalla **distribuzione delle responsabilità**, dalla disponibilità delle risorse e dal coordinamento tra i livelli operativi e gestionali.

Coerenza tra analisi e piano

Il piano deve essere **il riflesso fedele della BIA**. Ogni attività critica deve essere associata a misure proporzionate e attuabili.

Esempio: se un'attività ha un RTO di 4 ore, il piano non può prevedere una soluzione attivabile in 12. Se la perdita accettabile di dati è di un'ora, il sistema informatico deve garantire backup almeno ogni 60 minuti.

La coerenza tra analisi e piano è una condizione indispensabile per trasformare la strategia in operatività.

Monitoraggio, formazione e aggiornamento continuo

Un piano efficace è **conosciuto e praticato**. Non basta redigerlo: bisogna assicurarsi che le persone coinvolte:

- sappiano dove trovarlo;
- siano formate all'uso;
- lo abbiano testato in scenari realistici.

Ogni evento critico o esercitazione deve produrre un aggiornamento. Anche modifiche organizzative, nuove tecnologie o cambiamenti nei processi richiedono una revisione del piano.

Il piano vive solo se viene utilizzato, testato, aggiornato. È uno strumento dinamico, non un archivio.

7. Sintesi e riflessioni finali

Il percorso formativo sulla business continuity ha mostrato come garantire la continuità operativa non sia un semplice esercizio tecnico, ma una responsabilità trasversale, che coinvolge persone, strutture e cultura organizzativa. Dalla definizione dei ruoli all'elaborazione delle strategie, ogni elemento del sistema deve essere coerente, comprensibile e concretamente attuabile.

Cultura della resilienza e prontezza organizzativa

La resilienza non si improvvisa. È il risultato di un percorso che combina consapevolezza, preparazione e capacità di apprendere dagli eventi. Un'organizzazione pronta è quella che:

- ha identificato con chiarezza le sue attività essenziali;
- conosce i limiti temporali oltre i quali l'impatto diventa inaccettabile;
- ha formato le persone a reagire in modo coordinato e sicuro;
- ha diffuso una cultura in cui tutti si sentono coinvolti nella prevenzione e nella risposta.

Senza questa base culturale, anche il piano meglio scritto resta lettera morta.

Integrazione tra funzioni e ruoli

Il successo della continuità operativa dipende dalla **collaborazione tra figure diverse**: Incident Coordinator, RSPP, Direzione, responsabili tecnici, comunicazione. Nessuno può affrontare un evento critico da solo. Serve una visione condivisa, strumenti compatibili e una catena di decisione chiara.

La simulazione e la verifica aiutano a evidenziare:

- ambiguità nei ruoli;
- procedure mancanti o incoerenti;
- rischi organizzativi legati alla frammentazione delle competenze.

Investire nella collaborazione tra le funzioni è, a tutti gli effetti, una forma di prevenzione.

Il piano come strumento vivo

Il piano di business continuity non è il fine del percorso, ma il suo punto di partenza operativo. Serve a garantire:

- continuità nei servizi;
- sicurezza per le persone;
- protezione degli asset e della reputazione.

Perché sia efficace, deve essere:

- aggiornato regolarmente;
- comunicato a chi lo deve applicare;
- provato attraverso esercitazioni periodiche;
- migliorato dopo ogni evento reale o simulato.

La sua efficacia non si misura dalla complessità del documento, ma dalla **capacità dell'organizzazione di reagire con lucidità, efficacia e coerenza** a ciò che non si può prevedere.

Glossario dei termini chiave

- **Business Continuity:** capacità di un'organizzazione di mantenere o ripristinare le sue attività critiche durante e dopo eventi dirompenti.
- **Resilienza organizzativa:** abilità di un'organizzazione di adattarsi, assorbire gli shock e continuare a operare anche in condizioni avverse.
- **Issue:** evento circoscritto, gestibile con risorse ordinarie.
- **Incidente:** evento significativo, ma contenuto localmente attraverso risposte tempestive.
- **Crisi:** evento straordinario che compromette la continuità e richiede decisioni complesse.
- **Incident Coordinator:** figura operativa incaricata di gestire l'emergenza sul campo, attivando il piano e coordinando le risposte.
- **RSPP (Responsabile del Servizio Prevenzione e Protezione):** figura tecnica che valuta i rischi, propone misure preventive e supporta le scelte in fase di emergenza.
- **BIA (Business Impact Analysis):** analisi dell'impatto di un'interruzione sulle attività critiche, utilizzata per definire priorità e strategie.

- **MTPD (Maximum Tolerable Period of Disruption):** tempo massimo entro il quale un'attività deve essere ripristinata per evitare danni gravi.
- **RTO (Recovery Time Objective):** tempo obiettivo per ripristinare un'attività dopo l'interruzione.
- **RPO (Recovery Point Objective):** perdita di dati o produzione accettabile al momento della ripresa.
- **BCMS (Business Continuity Management System):** sistema documentato di gestione della continuità, strutturato secondo la norma ISO 22301.
- **PDCA (Plan-Do-Check-Act):** ciclo del miglioramento continuo su cui si basa la gestione del BCMS.

Appendice 1 – Schema logico di un BCMS secondo ISO 22301

1. **Contesto** → Analisi interna ed esterna, aspettative degli stakeholder
2. **Leadership** → Politica, ruoli, impegno
3. **Pianificazione** → Rischi, obiettivi, azioni
4. **Supporto** → Risorse, formazione, comunicazione
5. **Operatività** → Attività critiche, piani di continuità
6. **Valutazione** → Audit, indicatori, monitoraggio
7. **Miglioramento** → Azioni correttive, revisione

Appendice 2 – Esempi di strategie operative

- Backup dati giornalieri su cloud esterno
- Sedi alternative pronte all'uso per servizi critici
- Rete di fornitori secondari prequalificati
- Contratti attivabili in emergenza per logistica e supporto tecnico
- Linee guida per attivare lo smart working in 24 ore

Appendice 3 – Modello di check-list per l'analisi d'impatto

Attività	MTPD	RTO	RPO	Risorse critiche	Conseguenze attese	Priorità
Servizio X	48h	24h	1h	Server, personale	Operative, legali	Alta
Prodotto Y	72h	36h	4h	Fornitori, energia	Reputazionali	Media

Appendice 4 – Bibliografia essenziale e riferimenti normativi

- ISO 22301:2019 – *Security and resilience – Business continuity management systems – Requirements*
- ISO 22316:2017 – *Security and resilience – Organizational resilience – Principles and attributes*