

Corso NIS2 Advanced Business Continuity

Relatore: **Marcello Cutrone** (Business Continuity Manager - CSI Piemonte)

Alessandria, 19 maggio 2026



Obiettivi del corso



NIS2 e BC: le nuove direttive e il loro impatto sulla Continuità Operativa.

La Business Continuity: cos'è e perché è fondamentale.

Realizzare un PCO: linee guida per la creazione di un Piano di Continuità Operativa.

Caso Studio BIA: un esempio concreto di Business Impact Analysis.

Misure e Requisiti NIS2





NIS2 e Business Continuity: obblighi e opportunità

La Direttiva NIS2 rafforza gli obblighi di cybersecurity, ponendo maggiore enfasi sulla Business Continuity.

Punti Chiave che Richiamano la BC:

1. Politica e Procedura (GV.PO-01):

- Necessità di politiche documentate per la continuità operativa, il ripristino in caso di disastro e la gestione delle crisi.

2. Affidamento di Forniture (GV.SC-01):

- Gli accordi con i fornitori devono prevedere requisiti di continuità operativa e ripristino in caso di disastro, basati sui risultati della BIA.

3. Piani di Continuità Operativa (ID.IM-04):

- Obbligo di definire, attuare e aggiornare un Piano di Continuità Operativa documentato per i sistemi rilevanti, includendo finalità, ruoli, contatti, risorse (backup, ridondanze).

4. Salvaguardia dei Dati (PR.DS-11):

- Backup periodici di dati e configurazioni, con copie offline per i sistemi rilevanti, in accordo con le esigenze di BC e DR identificate nei piani.

Conclusione: NIS2 non è solo un obbligo, ma un'opportunità per rafforzare la resilienza operativa della tua organizzazione.

BC: Perché è Fondamentale





Business Continuity: la capacità di non fermarsi mai

La Business Continuity è la capacità di un'organizzazione di continuare a erogare prodotti e servizi essenziali, entro tempi accettabili e con una capacità produttiva predefinita, anche durante un'interruzione grave.

Perché è Cruciale?

Resilienza: essere preparati e reagire rapidamente agli eventi disastrosi.

Riduzione del Rischio: minimizzare l'impatto delle interruzioni.

Servizi Garantiti: mantenere l'erogazione dei servizi critici.

Conformità: soddisfare obblighi normativi (es. NIS2) e contrattuali.

Reputazione: fornire garanzie a clienti e stakeholder.

ISO 22301: Introduzione





ISO 22301: lo standard per la tua resilienza

La ISO 22301:2019 fornisce i requisiti per un Sistema di Gestione della Continuità Operativa (BCMS) su come **l'organizzazione deve governare, monitorare, controllare e migliorare** l'intero processo di continuità operativa.

Il BCMS è il **“framework organizzativo”** che assicura che il BCM sia:

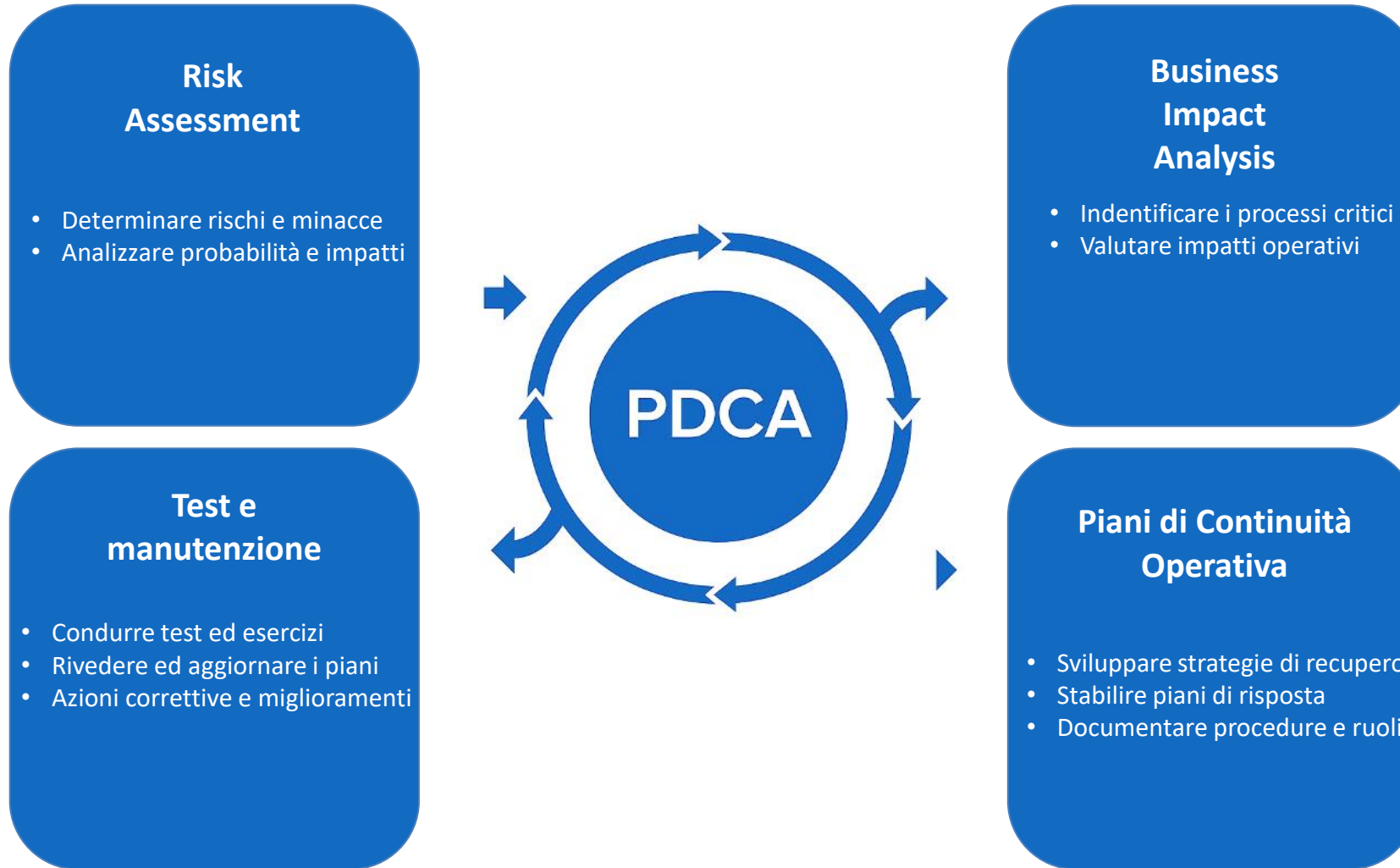
- ✓ **ripetibile**
- ✓ **governato**
- ✓ **misurato**
- ✓ **migliorato nel tempo**

Si fonda sul ciclo P-D-C-A per il Miglioramento Continuo:

- 1. Pianificare (Plan):** definire obiettivi e processi necessari.
- 2. Attuare (Do):** implementare i processi e i controlli.
- 3. Verificare (Check):** monitorare le prestazioni e analizzare i risultati.
- 4. Agire (Act):** migliorare continuamente il sistema.



ISO 22301: Lo Standard per la Tua Resilienza





ISO 22301:2019

La norma ISO 22301 definisce i requisiti per lo sviluppo di un efficace sistema di gestione della continuità operativa (BCMS).

Tale sistema definisce:

- Gli obiettivi per comprendere l'importanza dello sviluppo di un sistema di continuità operativa
- Come attuare e rendere operativi controlli per gestire la resilienza di un'organizzazione in seguito a fenomeni destabilizzanti
- Come monitorare e riesaminare le prestazioni e l'efficacia del BCMS
- Come migliorare l'efficacia del sistema continuamente

Tale sistema è caratterizzato dai seguenti **elementi chiave**:

- La politica del sistema
- Persone con responsabilità definite
- Processi di gestione relativi a: politica, pianificazione, attuazione e funzionamento, valutazione delle prestazioni, miglioramento, riesame degli organi direttivi
- Documentazione che fornisce evidenze modificabili
- Qualsiasi processo di gestione pertinente all'organizzazione



Business Continuity Management System (BCMS)

BCM

(Business Continuity Management)

Il contenuto (Analisi, piani, prove)

E' un processo gestionale che:

- ✓ permette di identificare le possibili minacce per l'organizzazione e gli impatti che avrebbero su di essa se si verificassero;
- ✓ permette di creare una strategia organizzativa volta alla sopravvivenza dell'organizzazione in caso di evento sfavorevole;
- ✓ salvaguarda gli interessi degli stakeholders dell'organizzazione fornendo una maggiore sicurezza di continuità operativa.

Obiettivo: la Resilienza Operativa

BCMS

(Business Continuity Management System)

Il contenitore (regole, ruoli, controlli, audit)

E' il sistema di gestione generale dell'organizzazione incentrato sulla continuità operativa, con lo scopo di:

- ✓ stabilire, implementare, controllare e migliorare continuamente il BCM;
- ✓ garantire il rispetto delle policy di continuità operativa dichiarate dall'organizzazione;
- ✓ dimostrare conformità ai terzi;
- ✓ ottenere una certificazione/registrazione del proprio BCMS da un ente certificatore terzo
- ✓ redigere un'auto-dichiarazione di conformità nel rispetto dell'ISO di riferimento.

Il BCM può esistere senza BCMS, ma **il BCMS non può esistere senza il BCM.**



RISCHIO E CONTINUITA' OPERATIVA: due facce della stessa medaglia

Risk Management:

- ✓ Identifica, analizza e valuta i rischi.
- ✓ Definisce le strategie di trattamento (mitigazione, accettazione, trasferimento, evitamento).
- ✓ Obiettivo: Ridurre la probabilità e l'impatto degli eventi avversi.

Business Continuity:

- ✓ Si concentra sulla capacità di recupero e resilienza.
- ✓ Sviluppa piani per continuare le operazioni in caso di interruzione.
- ✓ Obiettivo: Garantire la ripresa dei servizi entro tempi e livelli predefiniti.

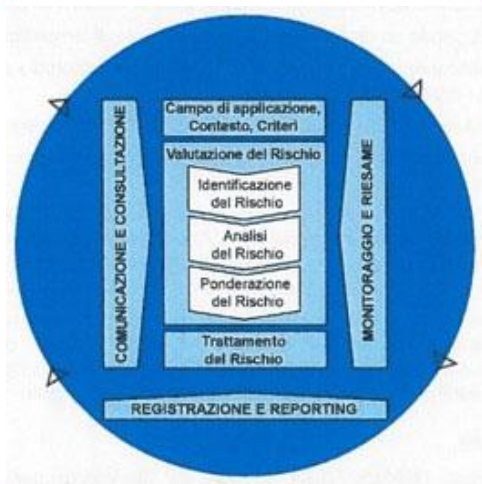
Insieme per la Resilienza Operativa!

Queste due discipline lavorano in sinergia per costruire un approccio olistico alla resilienza, garantendo che l'organizzazione sia non solo protetta, ma anche capace di adattarsi e ripartire.



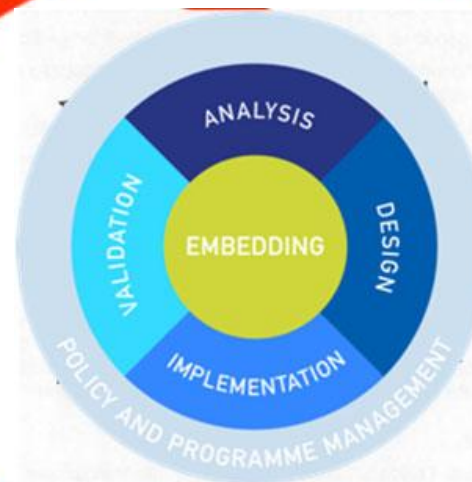
GESTIONE DEI RISCHI E CONTINUITA' OPERATIVA

1- Risk Management



lavorano insieme per
garantire resilienza
(approccio olistico)

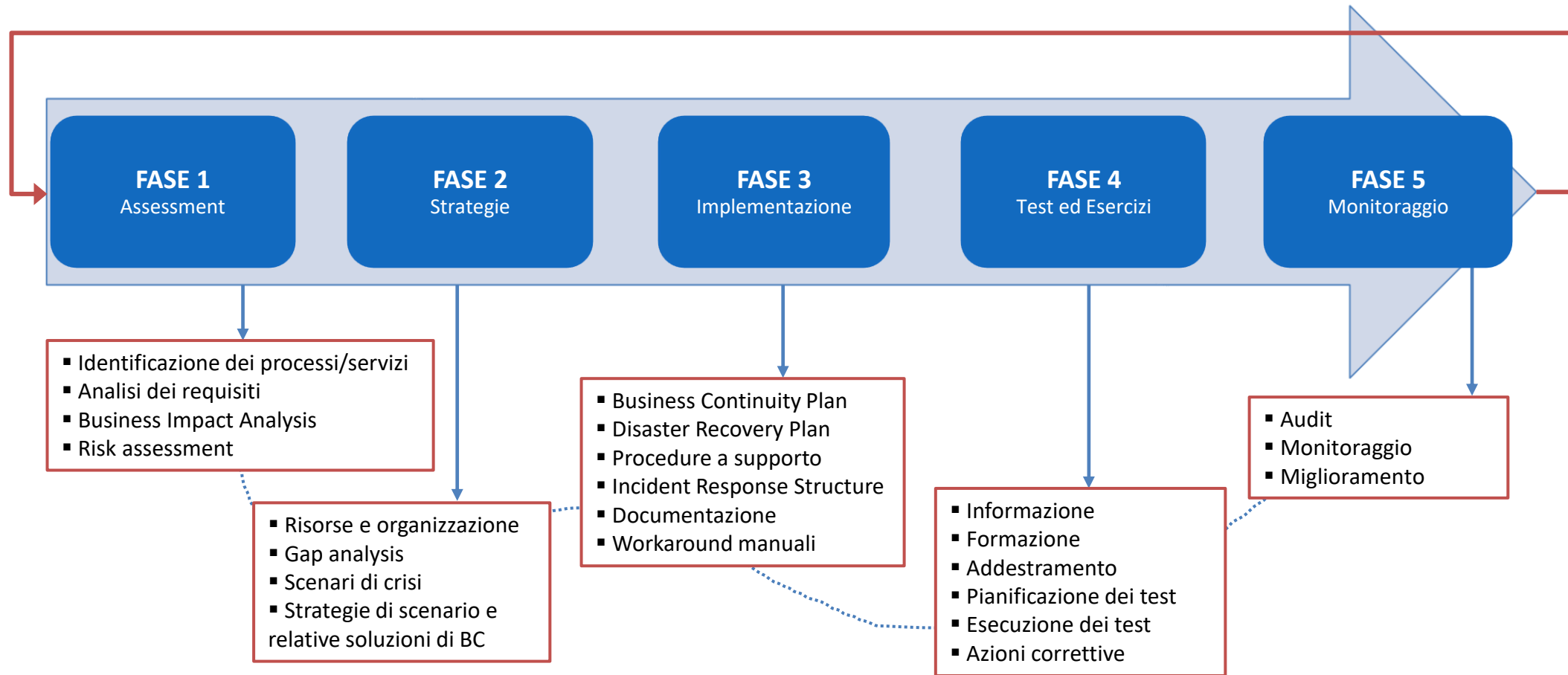
2- Business Continuity



adattamento continuo



BC nella ISO 22301: Processo iterativo





STANDARD METEOROLOGICI

Disaster Recovery International Institute" (DRI),
Business Continuity Institute" (BCI),
National Institute of Standards and Technology" (NIST),
Information Systems Audit and Control Association" (ISACA).

Tutte queste organizzazioni concordano sulla presenza del seguente set minimo di best practices quando si disegna e realizza un piano di business continuity:

- ✓ deve essere approvato un budget per il BCP da parte del top management;
- ✓ deve essere identificata una struttura che in caso di disastro o di interruzione del servizio coordini la strategia di ripristino;
- ✓ deve essere previsto un sistema per la gestione degli incidenti o comunque un processo per controllare la situazione ed operare il ripristino;
- ✓ il piano deve essere periodicamente rivisto.





STANDARD METOLOLOGICI: Disaster Recovery International Institute (DRI)

Area tematica 1 - Obiettivi - Gestione del Programma

1. Stabilire la necessità di un programma di continuità operativa
2. Ottenere supporto e finanziamenti per il programma di continuità operativa
3. Costruire il framework organizzativo a supporto del programma di continuità operativa
4. Introdurre concetti chiave, come la gestione del programma, la consapevolezza del rischio, l'identificazione di funzioni/processi critici, le strategie di recupero, la formazione e la consapevolezza, l'esercizio/test

Area tematica 2 Obiettivi - Analisi del Rischio

1. Identificare i rischi che possono influire negativamente sulle risorse o sull'immagine dell'organizzazione
2. Valutare i rischi per determinare i potenziali impatti sull'organizzazione, consentendo all'organizzazione di determinare l'uso più efficace delle risorse per ridurre tali potenziali impatti

Area tematica 3 Obiettivi - BIA

1. Identificare e dare priorità alle funzioni e ai processi dell'organizzazione al fine di accertare quali avranno il maggiore impatto nel caso in cui non fossero disponibili
2. Valutare le risorse necessarie per supportare il processo di analisi dell'impatto operativa
3. Analizzare i risultati per accertare eventuali lacune tra i requisiti dell'organizzazione e la sua capacità di soddisfare tali requisiti



STANDARD METOLOLOGICI: Disaster Recovery International Institute (DRI)

Settore Disciplinare 4 Obiettivo - Strategie di continuità operativa

1. Selezionare strategie efficaci in termini di costi per ridurre le carenze identificate durante i processi di valutazione del rischio e di analisi dell'impatto operativo (BIA).

Settore Disciplinare 5 Obiettivo - Preparazione e risposta agli incidenti

1. Sviluppare e assistere nell'implementazione di un sistema di gestione degli incidenti che definisca i ruoli organizzativi, le linee di autorità e la successione di autorità
2. Definire i requisiti per sviluppare e implementare il piano di risposta agli incidenti dell'entità
3. Garantire che la risposta agli incidenti sia coordinata con le organizzazioni esterne in modo tempestivo ed efficace, quando appropriato

Settore Disciplinare 6 Obiettivo - Sviluppo e implementazione del piano

1. Sviluppare, implementare e documentare i piani da utilizzare durante un incidente che consentiranno all'organizzazione di continuare a funzionare



STANDARD METOLOLOGICI: Disaster Recovery International Institute (DRI)

Settore Disciplinare 7 Obiettivo - Programma di sensibilizzazione e formazione

1. Stabilire e mantenere programmi di formazione e sensibilizzazione che consentano al personale di rispondere agli incidenti in modo calmo ed efficiente.

Settore Disciplinare 8 Obiettivo - Esercizio/test, valutazione e manutenzione del piano di continuità aziendale

1. Stabilire un programma di esercizi, valutazione e manutenzione per mantenere uno stato di prontezza.

Settore Disciplinare 9 Obiettivo - Crisis communication

1. Fornire un quadro di riferimento per lo sviluppo di un piano di comunicazione in caso di crisi
2. Garantire che il piano di comunicazione di crisi fornisca una comunicazione tempestiva ed efficace con le parti interne ed esterne

Settore Disciplinare 10 Obiettivo - Coordinamento con agenzie e risorse esterne

1. Stabilire politiche e procedure per coordinare le attività di risposta agli incidenti con gli enti pubblici.

Attività Operative BIA





BIA: misurare l'Impatto per agire

Cos'è una BIA?

È la tecnica fondamentale per valutare i requisiti di continuità operativa che determina:

- **Urgenza delle Attività:** quali sono i processi più critici?
- **Impatto delle Interruzioni:** quali conseguenze avrebbero sulla fornitura di prodotti e servizi?

Criteri di Valutazione degli Impatti:

- ✓ **Finanziario:** Perdite di profitti, multe, costi di ripristino.
- ✓ **Reputazionale:** Danno all'immagine, perdita di fiducia.
- ✓ **Legale/Normativo:** Sanzioni, violazioni di conformità.
- ✓ **Contrattuale:** Inadempienza con clienti e fornitori.

Benefici della BIA:

- ✓ Prioritizzazione chiara delle attività.
- ✓ Identificazione delle risorse necessarie.
- ✓ Base per definire strategie di recupero efficaci.



Processo di BIA

Analizza le conseguenze di un evento dirompente che coinvolge l'intera organizzazione, parte di essa o una terza parte esterna ad essa ma comunque collegata



Valuta quali processi potrebbero avere un maggiore impatto sull'operatività dell'organizzazione se non dovessero essere più disponibili



Esegue l'analisi dettagliata dei processi e delle attività aziendali per individuare le tempistiche e le risorse necessarie per far ripartire la produzione/il servizio interrotto



ISO 22317- guida per la BIA

La ISO 22317 è una guida che dettaglia come **Costruire**,
Implementare, **Mantenere** una BIA rispettando i requisiti
indicati nella ISO 22301:2019



Pianificazione – le BIA

BIA iniziale

Fornisce un'analisi di alto livello che può essere utilizzata per delineare un quadro per le BIA a maggior livello di dettaglio. Può anche essere utilizzata per precisare il campo di applicazione del programma di continuità operativa (tipicamente solo per la prima volta che un'organizzazione esegue una BIA).

BIA per i prodotti e servizi

Identifica e classifica in ordine di priorità i prodotti e i servizi e stabilisce i requisiti per la continuità operativa a livello strategico.

BIA per i processi

Determina i processi necessari per l'erogazione dei prodotti e dei servizi prioritari dell'organizzazione.

BIA per le attività

Individua e classifica in ordine di priorità le attività che forniscono i prodotti e i servizi più urgenti e stabilisce le risorse necessarie per la continuità di tali attività.



Pianificazione e gestione del processo



- ✓ Interne
- ✓ Esterne
- ✓ Terze parti



Possono esistere delle forti relazioni tra processi/strutture, fornitori, prodotti, risorse



Riassumiamo il Processo di BIA

1. Preparazione alla BIA

- Definizione Ambito e Obiettivi
- Ruoli, Responsabilità e Risorse
- Supporto del Top Management

2. Svolgimento della BIA

- Identificazione Attività Critiche
- Analisi Impatti e Dipendenze
- Validazione Risultati

3. Risultati e Azioni

- Definizione Strategie di Continuità Operativa



Monitoraggio e revisione

Generalmente il processo di BIA deve essere rivisto **annualmente** o a seguito di un **cambiamento organizzativo**.

Alcuni esempi:

- ✓ fusioni e acquisizioni;
- ✓ cambiamenti direzionali strategici;
- ✓ modifiche al prodotto o servizio;
- ✓ modifiche normative;
- ✓ modifiche contrattuali;
- ✓ cambiamenti operativi (ICT, supply chain, sito, struttura)
- ✓ lezioni derivanti da esercizi di Continuità Operativa o interruzioni.



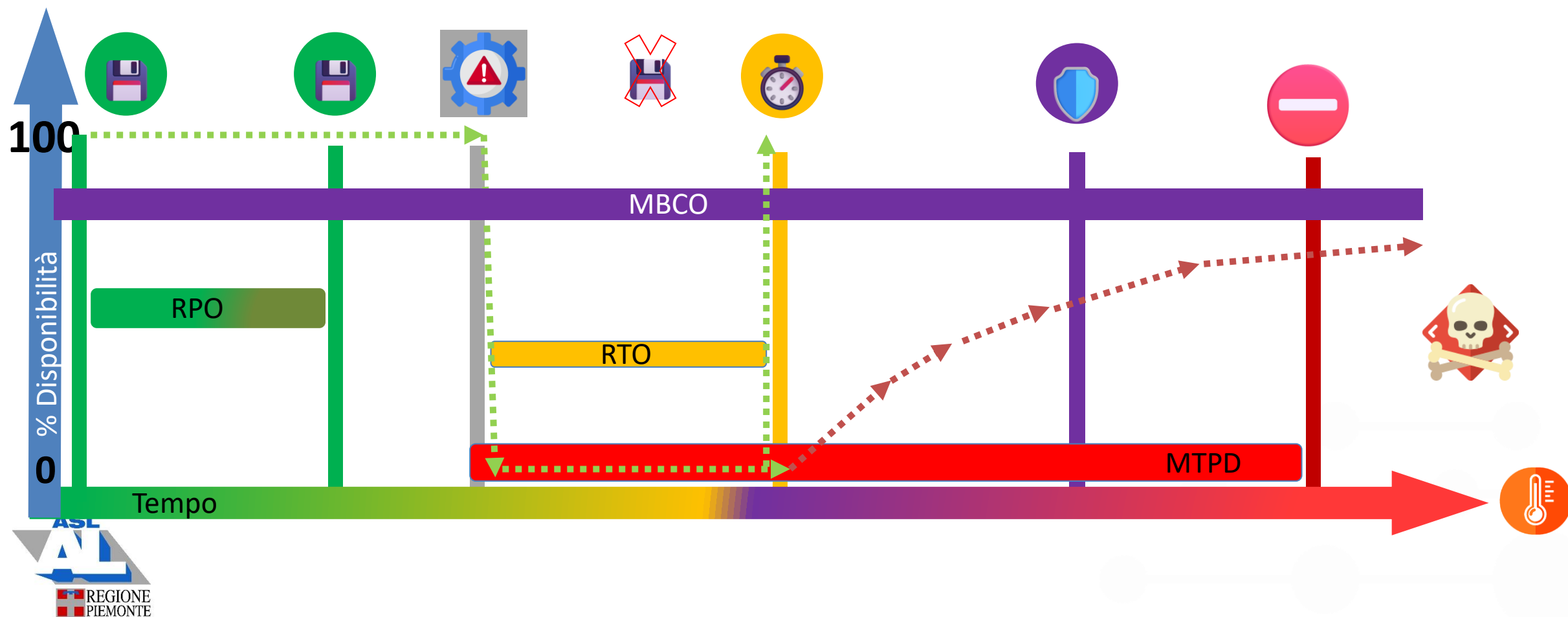
Grafico temporale dell'indisponibilità

RPO (Recovery Point Objective): massimo intervallo di dati perdibili.

RTO (Recovery Time Objective): tempo per ripristinare l'operatività.

MBCO (Minimum Business Continuity Objective): livello minimo di servizio accettabile.

MTPD (Maximum Tolerable Period of Disruption): oltre questo limite il business è compromesso.



Attività Operative Strategia





La determinazione e scelta di una strategia deve essere basata sui risultati dell'analisi di impatto sul business e della valutazione del rischio.

La Direzione Aziendale deve determinare una strategia appropriata per la continuità operativa, ai fini della:

- ✓ protezione delle attività prioritarie
- ✓ stabilità, continuità, ripresa e recupero
- ✓ mitigazione, reazione e gestione degli impatti.

La determinazione della strategia deve comprendere l'approvazione delle priorità da dare ai tempi per la ripresa delle attività (RTO – RPO) ed anche MBCO e MTPD.

La progettazione delle soluzioni relative alla modalità con cui un'organizzazione continuerà a operare a seguito di un'interruzione si basa sui requisiti di continuità operativa individuati nella BIA e sui risultati della valutazione dei rischi e delle minacce.

La scelta della soluzione è dettata non soltanto dal costo ma dall'importanza del valore espresso nell'RTO.

Esistono numerose e ben collaudate soluzioni di continuità operativa che è possibile utilizzare all'interno di un'organizzazione.



HOT SITE

Diversificazione

Separare attività e risorse su più sedi per garantire continuità operativa in caso di interruzione. È ideale quando l'RTO si misura in secondi, minuti o ore.

Replica

Duplicare risorse per una ripresa immediata. La sede replicata resta inattiva finché non deve assorbire le attività interrotte.

WARM SITE

Stand-by

Per RTO più lunghi (giorni), si utilizza un “warm site”, ovvero una struttura temporaneamente chiusa ma riattivabile rapidamente.

Acquisizione post-incidente

Per attività con RTO di giorni o settimane, le risorse vengono procurate solo dopo l'interruzione, basandosi su un elenco prioritario predefinito.

Nessuna azione

Si attende l'evento prima di decidere. Adatto quando l'RTO è di settimane o mesi o quando predisporre risorse in anticipo è impraticabile.



Determina le risorse necessarie per attuare le strategie definite, considerando alcune tipologie di risorse tipo:

- ✓ Persone
- ✓ Edifici, ambiente di lavoro e relativi servizi
- ✓ Impianti attrezzature e materiali di consumo
- ✓ Trasporti
- ✓ Risorse finanziarie
- ✓ Partner e fornitori

Per quanto riguarda i rischi identificati che richiedono un trattamento, l'organizzazione deve utilizzare misure proattive come ad esempio:

- ✓ Ridurre la probabilità di interruzione
- ✓ Abbreviare il periodo di interruzione
- ✓ Limitare l'impatto dell'interruzione sui servizi e prodotti chiave dell'organizzazione



ATTIVITA' OPERATIVE

Implementazione

- Business continuity Plan
- Disaster recovery Plan
- Procedure operative
- Incident response structure
- Documentazione a supporto
- Workaround manuali



BCPlan: Contenuti

1	SCOPO ED APPLICABILITA'	3
1.1	SCOPO.....	3
1.2	APPLICABILITA'	4
2	RIFERIMENTI NORMATIVI	5
3	TERMINI E DEFINIZIONI	5
4	RUOLI E RESPONSABILITA'	7
4.1	RESPONSABILITA' DEL PCOI	7
4.2	ORGANIGRAMMA DI EMERGENZA E GESTIONE DELLA CRISI	8
4.3	AREE, PROFILI ORGANIZZATIVI COINVOLTI E CONTACT LIST DEI REFERENTI.....	11
5	FORMAZIONE, INFORMAZIONE E DOCUMENTAZIONE	11
5.1	FORMAZIONE.....	12
5.2	INFORMAZIONE	12
5.3	DOCUMENTAZIONE A SUPPORTO	13
6	BIA E RISK ASSESSMENT	14
6.1	SCENARI DI CRISI	14
6.2	CRITERI MINIMI DI SICUREZZA E CONTROLLI ATTUATI NEL SITO SECONDARIO	18
7	STRATEGIA DI CONTINUITA' OPERATIVA E RISORSE IMPIEGATE.....	18
7.1	RANK DI PRIORITA' DI RIPRISTINO.....	20
7.2	FASE DI EMERGENZA	22
7.3	FASE DI CRISI.....	24
7.4	FASE DI RIENTRO.....	24
7.5	STRATEGIE DI SCENARIO	25
7.6	STRATEGIA DI COMUNICAZIONE	33
8	PROCEDURA DI GESTIONE DELLA CRISI	33
8.1	FASE 0 – RILEVAZIONE DELL'EVENTO	34
8.2	FASE 1 – STATO DI EMERGENZA.....	36
8.3	FASE 2 – STATO DI CRISI	37
8.3.1	CRISIS ASSESSMENT	37
8.3.2	CRISIS RESPONSE.....	39
8.4	FASE 3 – RIENTRO ALLA NORMALITA' OPERATIVA	40
9	TEST ED ESERCIZI	40
10	ESERCIZIO E GESTIONE DEI CHANGE	40
11	ALLEGATI.....	41
11.1	MODULISTICA.....	41
11.2	LISTE	41
11.3	PROCEDURE TECNICHE	42
11.4	SCENARI.....	42
	FLUSSO DI GESTIONE DELLA CRISI	44



Allegati al BCPlan: esempi

- ✓ Procedure organizzative
- ✓ Procedure di ripristino dei sistemi informativi
- ✓ Contact list fornitori essenziali
- ✓ Contact list personale
- ✓ Piano della comunicazione
- ✓ Moduli predefiniti da utilizzare durante la crisi
- ✓ Piano delle esercitazioni e dei test
- ✓ Incident response structure



Fase 4 – Esercitazioni e Test

- Comunicazione
- Formazione e Addestramento
- Pianificazione dei Test
- Esecuzione dei test
- Azioni correttive



Fase 5 - Monitoraggio

- Audit
- Monitoraggio
- Miglioramento



Gestione della crisi: dal rilevamento al ritorno alla normalità

Le 5 Fasi della Crisi

1. Fase 0: Rilevazione

- Identificazione dell'evento e della sua gravità.

2. Fase 1: Gestione dell'Emergenza

- Risposta immediata, messa in sicurezza.

3. Fase 2: Gestione della Crisi (Assessment & Response)

- Valutazione dettagliata dell'impatto e attivazione delle strategie.

4. Fase 3: Ritorno alla Normalità Operativa

- Progressivo ripristino dei servizi e delle funzionalità.

Cosa Fare:

Durante la Crisi	Dopo la Crisi
Mantenere la calma e attivare il team di crisi.	Dichiarare la fine della crisi.
Trasparenza: Fornire aggiornamenti costanti.	Analisi Causa Radice (Root Cause Analysis).
Focus sull'RTO: Anche con soluzioni temporanee.	Report post-mortem: Condividere le lezioni apprese.
Supportare il personale e i clienti.	Azioni Correttive: Implementare miglioramenti.
Cooperare con le autorità.	Revisione: Aggiornare piani e procedure.



Scenari di crisi

INDISPONIBILITA' DEI LOCALI

I luoghi di lavoro o parte di esse sono inagibili e, pertanto, indisponibili ad essere utilizzati.

INDISPONIBILITA' DEI FORNITORI CRITICI

I fornitori critici non sono disponibili nei tempi necessari per garantire la continuità del business.

INDISPONIBILITA' DELLE UTILITIES

Le utilities (energia, acqua, riscaldamento, ecc) non sono disponibili e compromettono la normale erogazione dei servizi di business.

INDISPONIBILITA' DELLE PERSONE

Le persone chiave o critiche sono indisponibili e la loro assenza pregiudica la corretta disponibilità dei servizi di business.

INDISPONIBILITA' DELLA DOCUMENTAZIONE ESSENZIALE

La documentazione operativa essenziale è indisponibile e questo pregiudica la corretta erogazione dei servizi di business.



EVENTI | Comprendiamone la gravità

LE FASI DELLA CRISI

FASE 0: Rilevazione

FASE 1: Gestione dell'emergenza

FASE 2: Gestione della crisi

— **FASE 2.1** - Crisis Assessment

FASE 2.2 - Crisis Response

FASE 3: Ritorno alla normalità operativa

LIVELLO GRAVITA'	DESCRIZIONE E TRIGGER
CRITICO (obbligo di dichiarare la crisi)	Incidente che causa interruzione dei servizi critici e che è caratterizzato da <u>almeno uno</u> di questi elementi: - Durata dell'indisponibilità > RTO previsto - Potenziale superamento del MTPD previsto - Impatto prolungato su più servizi critici su larga scala - Rischio concreto di incolumità delle persone - Necessità di attivare il sito di DR
GRAVE (obbligo di dichiarare la crisi)	Incidente che causa degrado o interruzione dei servizi critici e che è caratterizzato da <u>almeno uno</u> di questi elementi: - Numero elevato di clienti coinvolti - Possibile mancato rispetto di SLA contrattuali - L'evento può causare anche in via potenziale l'arresto di uno o più servizi critici con effetto domino - L'evento non è risolvibile con mezzi ordinari e richiede il dispiegamento di risorse elevate e/o non quantificabili al momento - I locali sono fortemente compromessi - Significativi rischi per la sicurezza delle persone o delle informazioni - Disservizio stimabile > 2 ore e con potenzialità di superare il valore previsto di RTO - Potenziale necessità di attivare il sito di DR
MEDIO (crisi da valutare)	Incidente che causa degrado o interruzione dei servizi NON critici e che è caratterizzato da <u>almeno uno</u> di questi elementi: - Numero contenuto di clienti coinvolti - Non è a rischio il rispetto di SLA contrattuali - Continuità operativa del CSI Piemonte non a rischio a seguito dell'evento - Locali parzialmente compromessi - E' possibile risolvere l'incident con mezzi ordinari (procedura di incident) - Rischi per la sicurezza delle persone - Disservizio stimabile > 1 ora ma non ha potenzialità di superare il valore previsto di RTO
ORDINARIO	Incidente che causa degrado o interruzione dei servizi NON critici e che è caratterizzato da <u>almeno uno</u> di questi elementi: - Il disservizio non è significativo ed è limitato nell'estensione di clienti coinvolti - E' possibile risolvere l'incident con mezzi ordinari (procedura di incident) - I locali non sono compromessi - Non vi sono rischi per la sicurezza delle persone



SFATIAMO I MITI sulla Business Continuity

Mito 1: "Ho già il backup, sono a posto!"

Realtà: Il backup è cruciale per il *recupero dei dati (RPO)*, ma non garantisce la *continuità operativa (RTO)*. Serve un piano per riattivare i servizi!

Mito 2: "Ho doppia alimentazione e UPS, sono super continuo!"

Realtà: Questa è *alta affidabilità di sito*, non *Business Continuity*. Un evento più ampio (es. incendio) potrebbe compromettere l'intera sede.

Mito 3: "Ho un piano di Disaster Recovery, quindi sono tranquillo!"

Realtà: Il Disaster Recovery è una *misura tecnica* all'interno di un *Piano di Business Continuity*. Non vive da solo e si concentra sul recupero IT, non sull'operatività generale.

Mito 4: "Ho fatto la BIA di un servizio IT, so tutto!"

Realtà: La BIA valuta l'impatto sul *business*, non solo sull'IT. Hai considerato tutti i processi impattati, le dipendenze e i requisiti legali/contrattuali?

Mito 5: "Ho il mio team di Incident Response, sono invincibile!"

Realtà: E se i membri chiave sono assenti? Hai sostituti, contatti rapidi e coinvolgi anche i fornitori? Il team deve essere pronto e consapevole!



TERMINI CHIAVE DELLA BUSINESS CONTINUITY

Glossario Essenziale per la Continuità

Business Continuity

Insieme di soluzioni tecnico-organizzative attuate per garantire i requisiti di continuità definiti (RTO, RPO, MTPD, MBCO).

Requisito

Esigenza o aspettativa che può essere esplicitata, generalmente implicita, oppure obbligatoria.

Business Impact Analysis: Analisi di impatto operativa

Il processo di identificazione e valutazione degli impatti che un'interruzione di attività può avere su un'organizzazione.

Risorse

Tutti gli asset (equipaggiamento tecnico compreso), personale, capacità, tecnologie, siti di lavoro, forniture e informazioni (elettroniche o meno) di cui un'organizzazione ha bisogno per lavorare e per raggiungere i propri obiettivi.

Strategia

Insieme di soluzioni tecniche e organizzative per raggiungere gli obiettivi definiti con la BIA.

Fornisce le indicazioni per la stesura del piano e delle procedure di continuità.

Business Continuity Plan

Informazioni documentate che riguardano un'organizzazione al fine di rispondere a un'interruzione e riprendere, recuperare e ripristinare l'erogazione di prodotti e servizi coerentemente con i suoi obiettivi per continuità operativa.



TERMINI CHIAVE DELLA BUSINESS CONTINUITY

Glossario Essenziale per la Continuità

RTO (Recovery Time Objective):

- **Definizione:** Il tempo massimo desiderato entro cui i prodotti, i servizi o le funzioni devono essere ripristinati dopo un'interruzione.
- **Significato:** Quanto tempo possiamo permetterci di stare fermi?

RPO (Recovery Point Objective):

- **Definizione:** Massimo intervallo di dati perdibili.
- **Significato:** Quanta perdita di dati siamo disposti a tollerare?

MTPD (Maximum Tolerable Period of Disruption):

- **Definizione:** Il periodo massimo tollerabile di durata di un'interruzione, oltre il quale i danni diventerebbero inaccettabili.
- **Significato:** Il "punto di non ritorno" per il business.

MBCO (Minimum Business Continuity Objective):

- **Definizione:** Il livello minimo di funzionamento dei prodotti/servizi che deve essere garantito durante un'interruzione.
- **Significato:** Qual è il livello minimo di servizio che dobbiamo mantenere attivo?

Esempio di BIA



Grazie

marcello.cutrone@csi.it