Business Continuity (BC)

La Business Continuity (BC), o Continuità Operativa, è un approccio organizzativo strutturato finalizzato a garantire che un'organizzazione sia in grado di continuare a svolgere le proprie attività critiche a un livello accettabile anche in presenza di eventi avversi o interruzioni impreviste.
La BC non si limita alla gestione delle emergenze informatiche, ma coinvolge l'intera organizzazione, includendo persone, processi, infrastrutture, fornitori e comunicazione.

Elementi chiave della Business Continuity

- **Business Impact Analysis (BIA)**: identifica i processi aziendali critici e valuta l'impatto di un'interruzione sul business.
- **Valutazione dei rischi**: analizza minacce e vulnerabilità che possono compromettere la continuità operativa.
- **Strategie di continuità**: definiscono le soluzioni organizzative e operative per mantenere o ripristinare le attività essenziali.
- **Business Continuity Plan (BCP)**: documenti che descrivono ruoli, responsabilità, procedure operative, comunicazione ed escalation in caso di crisi.
- **Test ed esercitazioni**: verificano l'efficacia dei piani e ne garantiscono l'aggiornamento nel tempo.

La Business Continuity è un processo continuo orientato alla resilienza organizzativa e richiede il coinvolgimento del top management e di tutti i dipartimenti aziendali.

Disaster Recovery (DR)

Il Disaster Recovery (DR) è l'insieme delle misure, dei processi e delle procedure finalizzate al ripristino dei sistemi informativi e delle infrastrutture tecnologiche a seguito di un evento distruttivo o di una grave interruzione.

A differenza della Business Continuity, che adotta un approccio globale e organizzativo, il Disaster Recovery è focalizzato principalmente sull'ambito **ICT**.
Il DR ha l'obiettivo di garantire la disponibilità, l'integrità e la continuità dei servizi informatici necessari al supporto delle attività aziendali; esso si concentra sul recupero di risorse quali server, reti, applicazioni, dati e sistemi di storage, riducendo al minimo l'impatto delle interruzioni tecnologiche sul business.

Componenti chiave del Disaster Recovery
- **Recovery Time Objective (RTO)**: definisce il tempo massimo accettabile entro cui un sistema o servizio deve essere ripristinato.
- **Recovery Point Objective (RPO)**: indica la quantità massima di dati che l'organizzazione può permettersi di perdere in caso di incidente.
- **Strategie di ripristino**: includono backup, replica dei dati, ridondanza delle infrastrutture e utilizzo di siti alternativi.
- **Disaster Recovery Plan (DRP)**: documento che descrive le procedure tecniche e operative per il ripristino dei sistemi informativi.
- **Test e verifiche periodiche**: attività di simulazione e controllo per assicurare l'efficacia delle soluzioni di ripristino.

Il Disaster Recovery è una componente fondamentale della Business Continuity, poiché il ripristino tempestivo dei sistemi ICT rappresenta un prerequisito essenziale per la ripresa delle attività aziendali critiche.

ICT Readiness for Business Continuity

L'ICT Readiness for Business Continuity (IRBC) è il concetto che descrive il livello di preparazione delle tecnologie dell'informazione e della comunicazione (ICT) nel supportare la continuità operativa di un'organizzazione.

Secondo la norma ISO/IEC 27031, l'IRBC fornisce un quadro di riferimento per garantire che le risorse ICT siano adeguatamente progettate, gestite e mantenute al fine di sostenere i processi di Business Continuity e Disaster Recovery.
L'IRBC si colloca come elemento di collegamento tra Business Continuity e Disaster Recovery, assicurando che i requisiti di continuità del business siano correttamente tradotti in requisiti tecnologici.
In questo contesto, la preparazione dell'ICT non riguarda solo il ripristino dei sistemi, ma anche la loro capacità di prevenire, assorbire e reagire efficacemente alle interruzioni.

Principi fondamentali dell'ICT Readiness
- Allineamento con il business: le soluzioni ICT devono essere progettate in funzione delle esigenze di continuità dei processi aziendali critici.
- Approccio basato sul rischio: la preparazione ICT deve tenere conto delle minacce e delle vulnerabilità che possono compromettere la disponibilità dei servizi informativi.
- Definizione di requisiti di continuità ICT: i requisiti tecnologici devono essere coerenti con gli obiettivi di ripristino stabiliti dal business (RTO, RPO).
- Integrazione con BC e DR: l'IRBC deve essere pienamente integrata nei piani di Business Continuity e Disaster Recovery.
- Prevenzione e resilienza: l'ICT deve essere progettata per ridurre la probabilità e l'impatto delle interruzioni, non solo per reagire a esse.
- Test, manutenzione e miglioramento continuo: la preparazione ICT deve essere verificata regolarmente tramite test ed esercitazioni e aggiornata nel tempo.
L'ICT Readiness for Business Continuity consente all'organizzazione di garantire che le infrastrutture tecnologiche siano in grado di supportare efficacemente la continuità operativa, riducendo il rischio di interruzioni prolungate e assicurando una risposta strutturata agli eventi critici.

Aspetto	Business Continuity (BC)	Disaster Recovery (DR)
Definizione	Approccio olistico per mantenere le operazioni aziendali durante e dopo interruzioni	Piano specifico per ripristinare sistemi IT e infrastrutture tecnologiche dopo un disastro
Ambito	Tutti gli aspetti dell'organizzazione (persone, processi, tecnologia, strutture)	Principalmente infrastruttura IT e dati
Obiettivo principale	Garantire la continuità delle funzioni aziendali critiche	Ripristinare sistemi IT e dati dopo un disastro
Tempistica	Continuativa (prima, durante e dopo un'interruzione)	Principalmente post-disastro
Responsabilità	Coinvolge tutti i dipartimenti e il top management	Principalmente responsabilità del dipartimento IT
Pianificazione	Strategica e operativa, multidisciplinare	Tecnica e procedurale, focalizzata su IT
Focus sulla prevenzione	Alto - include strategie di mitigazione dei rischi	Medio - si concentra più sul ripristino che sulla prevenzione
Metriche chiave	KPI aziendali (impatto finanziario, reputazionale, operativo)	RPO (Recovery Point Objective), RTO (Recovery Time Objective)
Test e manutenzione	Esercitazioni aziendali complete, coinvolgimento di tutti i dipartimenti	Test tecnici dei sistemi di backup, procedure di restore
Durata implementazione	Processo a lungo termine, continuativo	Può essere implementato più rapidamente, focalizzato
Costi	Generalmente più elevati - coinvolge multiple risorse e dipartimenti	Più contenuti - focalizzati su tecnologia e infrastruttura IT

CONCLUSIONE

Business Continuity, Disaster Recovery e ICT Readiness rappresentano tre pilastri complementari della resilienza organizzativa.

La Business Continuity fornisce la visione strategica complessiva, orientata alla salvaguardia dei processi aziendali critici, mentre il Disaster Recovery mette a disposizione le capacità tecniche necessarie al ripristino dei sistemi informativi e delle infrastrutture tecnologiche.

L'ICT Readiness for Business Continuity garantisce che l'infrastruttura ICT sia costantemente preparata, resiliente e allineata agli obiettivi di continuità del business.

Un'organizzazione matura in termini di resilienza deve sviluppare questi tre ambiti in modo integrato e coerente, assicurando che le strategie di Business Continuity guidino le implementazioni di Disaster Recovery e ICT Readiness.

Allo stesso tempo, le soluzioni tecniche e i risultati delle attività di test e verifica forniscono un feedback continuo per il miglioramento della strategia complessiva;solo attraverso un approccio olistico e integrato è possibile raggiungere una resilienza organizzativa efficace, in grado di affrontare in modo strutturato le sfide e le incertezze del contesto operativo moderno.