CS0424IT — ESERCITAZIONE S9L2
BUSINESS CONTINUITY & DISASTER RECOVERY

Simone La Porta

GitHub

---

23 luglio 2024

1 TRACCIA

Durante la lezione teorica, abbiamo affrontato gli argomenti riguardanti la business continuity e disaster recovery. Nell'esempio pratico di oggi, ipotizziamo di essere stati assunti per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia.

Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la perdita annuale che subirebbe la compagnia nel caso di:

- Inondazione sull'asset «*edificio secondario*»
- Terremoto sull'asset «*datacenter*»
- Incendio sull'asset «*edificio primario*»
- Incendio sull'asset «*edificio secondario*»
- Inondazione sull'asset «*edificio primario*»
- Terremoto sull'asset «*edificio primario*»

DATI

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

2 INTRODUZIONE

2.1 *Pianificazione e scopo*

2.1.1 Analisi strutturata dell'organizzazione e del suo business

Un'analisi strutturata dell'organizzazione e del business dell'organizzazione è il primo passo nella stesura di un piano di continuità. In questa fase, lo scopo è quello di dettagliare e «mappare» i dipartimenti interni di una compagnia e gli individui con i servizi critici erogati dalla compagnia stessa. Infatti, in ottica di evento catastrofico, un piano di continuità ben strutturato dovrà, come prima priorità, ridurre gli impatti su quelli che sono i «servizi core», ovvero i servizi principali erogati dalla compagnia. Come abbiamo visto nelle unità precedenti per l'implementazione delle «remediation action», si riprende anche in questo contesto il concetto di «priorità»: gli asset critici, relativi al business hanno sempre la priorità.

2.1.2 Creazione di un Team

La creazione di un team / gruppo di lavoro responsabile del BCP che deve essere approvato dai dirigenti della compagnia stessa: il secondo step nello sviluppo di un piano d'azione per la continuità del business è l'identificazione delle persone responsabili del business continuity plan (BCP). Questa fase è molto importante, in quanto bisogna assicurare che tutti i dipartimenti di una compagnia siano consapevoli dell'esistenza di un piano di continuità. Pertanto, nella pianificazione del team di lavoro bisognerà includere:

- Un rappresentante di ogni dipartimento dell'organizzazione che si occupa di erogare servizi critici;
- Un esperto di servizi IT (information technology) con competenze tecniche nelle aree coperte dal BCP;
- Un membro del team di Cyber Security, che abbia competenze del processo BCP;
- Un membro del team della sicurezza fisica;
- Dei membri del team legale, che abbiano competenze sulle regolamentazioni, leggi e contratti in essere;

- Dei membri del team delle risorse umane (HR – human resources), per la gestione di eventuali impatti sullo staff, o su impiegati;
- Un rappresentante dei dirigenti che abbia potere decisionale, al fine di definire le priorità ed allocare eventualmente risorse.

2.1.3 Valutazione delle risorse ed asset disponibili

Una valutazione delle risorse ed asset disponibili che saranno incluse nelle attività di business continuity: una volta che il team responsabile del BCP è stato definito, è il momento di definire le risorse richieste dal BCP. Si possono definire le risorse definite per le tre fasi di seguito del BCP:

1. Sviluppo del BCP: (ovvero il costo) è perlopiù imputabile a capitale umano quale il team coinvolto nel processo di BCP ed eventualmente il costo dello staff esterno richiesto a supporto (se necessario).
2. Test, manutenzione e training per gli impiegati: il BCP deve essere testato, manutenuto, ma soprattutto bisogna organizzare delle sessioni di training / lezioni per gli impiegati al fine di mostrare il funzionamento del BCP.
3. Implementazione del BCP: infine, in caso di disastro, il BCP deve essere attuato il che richiede non solo capitale umano, ma anche un uso di risorse e mezzi. In questa fase, è molto probabile che per un periodo limitato una buona porzione della compagnia sia impegnata nell'implementazione del piano di continuità.

2.1.4 Analisi delle leggi e regolamentazioni

Un'analisi delle leggi e regolamentazioni che la compagnia deve rispettare. Ad esempio, potrebbero essere in vigore delle leggi che stabiliscono quali servizi devono essere sempre erogati anche in situazioni critiche da una data compagnia: capita piuttosto frequentemente, che le compagnie sono in qualche modo legate a leggi statali o regolamentazioni che governano l'implementazione dei piani di continuità. Questo succede spesso nel mercato dei «Financial Services», ovvero il mercato di quelle compagnie che erogano servizi finanziari come banche ed assicurazioni. In questi casi, le regolamentazioni pongono dei limiti o degli obblighi nello sviluppo dei piani di continuità operativa, ed è di conseguenza fondamentale capire il contesto

giuridico nel quale si posiziona la compagnia al fine di sviluppare un piano che sia in linea con le leggi e le regolamentazioni in vigore.

2.2 *Business Impact Analysis (BIA)*

Una volta completato il primo step della pianificazione, è tempo di affrontare il Business impact analysis (BIA), ovvero l'analisi degli impatti sul business. Il BIA ha lo scopo principale di identificare le risorse critiche di una compagnia e le potenziali minacce alle quali esse sono esposte. Inoltre, il BIA ha lo scopo di misurare la probabilità che tali minacce possano verificarsi e l'impatto che esse potrebbero avere sul business. Il BIA e conseguentemente la sua «misurazione» può seguire due approcci:

1. Qualitativo: per il calcolo degli impatti di determinate minacce sul business NON si prendono in considerazione parametri misurabili, o numerici, ma bensì l'analisi è guidata da fattori non numerici.

2. Quantitativo: il calcolo degli impatti sul business prende in considerazione solamente parametri numerici o quantificabili.

2.2.1 Identificazione delle priorità

Il primo task da eseguire quando ci si prepara ad affrontare un BIA è l'identificazione delle priorità del business. Questo fattore dipende ovviamente da quello che è lo scopo principale, o il business principale della compagnia. Da un punto di vista qualitativo, si potrebbero, di fatto, identificare le priorità in base alla loro criticità relativamente al business– dove agli asset a supporto del business viene assegnata una priorità superiore. Da un punto di vista quantitativo, si potrebbe invece creare una lista contenente tutti gli asset della compagnia ed assegnare ad ognuno di essi un valore monetario, chiamato «asset value» (AV) e successivamente assegnare una priorità in base al valore.

2.2.2 Identificazione dei rischi

Identificazione dei rischi: una volta completata la fase di identificazione delle priorità, bisogna stimare il rischio che impatterebbe l'organizzazione in caso di disastro. Possiamo dividere i rischi in due grosse categorie:

1. Disastri naturali: ricadono all'interno di questa categoria tutti quei fenomeni che non sono causati direttamente dall'uomo in prima persona, come ad esempio terremoti, maremoti, valanghe, eruzioni vulcaniche.

2. Disastri causati dall'uomo: in maniera complementare sono inclusi nei disastri causati dall'uomo tutti quei fenomeni che vedono l'uomo commettere un'azione in prima persona come atti terroristici, esplosioni etc.

2.2.3 Valutazione della probabilità

Una volta identificati i rischi che possono impattare sull'organizzazione, ad ognuno di essi si associa la probabilità che l'evento si verifichi. Se la probabilità è stimata in numero di volte che l'evento si è verificato nel corso di un anno, si parla di «Annualized Rate of Occurrence» (ARO), ovvero tasso annuale di occorrenza. I dati storici e le statistiche messe a disposizione degli enti pubblici possono sicuramente supportare la valutazione delle probabilità per quanto riguarda i disastri naturali.

2.2.4 Valutazione degli impatti

A valle dell'identificazione dei rischi e della probabilità che essi si verifichino, si può procedere con la fase di valutazione degli impatti. Il risultato della fase di valutazione degli impatti è una misura qualitativa (basso, medio, alto) o quantitativa (e quindi espressa in forma monetaria) degli impatti sul business legati ad un determinato evento.

2.3 *Business Planning*

Le prime due fasi del BCP si focalizzano sulla pianificazione del BCP e sull'identificazione delle priorità e dei rischi per il business. La fase del continuity planning ha invece lo scopo di sviluppare ed implementare una strategia per la riduzione dell'impatto dei rischi sugli asset protetti. Possiamo identificare all'interno della fase di continuity planning, le seguenti sottofasi:

1. Sviluppo della strategia: lo sviluppo della strategia è un'attività complementare all'identificazione delle priorità, discussa nella fase di BIA. Infatti, se nella BIA si identificano rischi ed asset prioritari, nella fase di sviluppo strategia si decidono i rischi che verranno gestiti all'interno del BCP. In questa fase il management deciderà quali rischi potrebbero

essere accettabili, e quali invece no, quali rischi sono da evitare e quali invece inserire all'interno del BCP.

2. Stesura dei processi: all'interno di questa fase vengono dettagliati i processi e le procedure da seguire per la salvaguardia degli asset critici: personale, edifici ed infrastrutture. È bene ricordare che le persone sono sempre «l'asset» più significativo di una compagnia e pertanto devono essere dettagliati i processi per assicurare l'incolumità durante un'emergenza.

2.4 *Approvazione ed Implementazione*

Una volta completate le fasi precedenti, è il momento di sottoporre il piano all'attenzione della dirigenza per revisione ed approvazione, prima di passare alla fase di implementazione, dove il team responsabile del BCP deve assicurarsi che tutte le risorse necessarie siano disponibili e che è stato organizzato, o erogato un piano di training per tutti gli impiegati che prendono attivamente parte al BCP. Infine, tutte le fasi precedenti devono essere ampiamente documentate e rese disponibili per eventuale consultazione da parte degli impiegati.

3 SVOLGIMENTO

In questo caso studio, analizziamo l'impatto di vari disastri su diversi asset di una compagnia.

3.1 *Inondazione sull'asset «Edificio Secondario»*

- **AV (Asset Value):** valore totale dell'asset, che per l'asset edificio secondario è pari a 150.000€.
- **EF (Exposure Factor):** percentuale di perdita dell'asset in caso di disastro, che per la coppia edificio secondario/inondazione è pari al 40%.
- **SLE (Single Loss Expectancy):** l'aspettativa di perdita singola, AV ∗ EF

$$\text{SLE} = 150.000\,€ \times 40\% = 60.000\,€$$

- **ARO (Annualized Rate of Occurrence):** il numero di volte che un evento si verifica in un anno, che per l'evento «Inondazione» è 1 volta ogni 50 anni, che equivale a 0.02 volte/anno.
- **ALE (Annualized Loss Expectancy):** l'aspettativa di perdita annualizzata, SLE ∗ ARO

$$\text{ALE} = \text{SLE} \times \text{ARO} = 60.000\,€ \times 0.02 = 1.200\,€$$

Dati Rilevanti

Parametro	Formulario	Calcolo	Valore
AV (Asset Value)			150.000€
EF (Exposure Factor)			40%
ARO (Annualized Rate of Occurrence)	$\frac{1}{50\text{ anni}}$		0.02
SLE (Single Loss Expectancy)	AV × EF	150.000 € × 40%	60.000€
ALE (Annualized Loss Expectancy)	SLE × ARO	60.000 € × 0.02	1.200€

3.2 *Terremoto sull'asset «Datacenter»*

- **AV (Asset Value):** valore totale dell'asset, che per l'asset datacenter è pari a 100.000€.
- **EF (Exposure Factor):** percentuale di perdita dell'asset in caso di disastro, che per la coppia datacenter/terremoto è pari al 95%.
- **SLE (Single Loss Expectancy):** l'aspettativa di perdita singola, AV ∗ EF

$$\text{SLE} = 100.000\,€ \times 95\% = 95.000\,€$$

- **ARO (Annualized Rate of Occurrence):** il numero di volte che un evento si verifica in un anno, che per l'evento «Terremoto» è 1 volta ogni 30 anni, che equivale a 0.033 volte/anno.
- **ALE (Annualized Loss Expectancy):** l'aspettativa di perdita annualizzata, SLE ∗ ARO

$$\text{ALE} = \text{SLE} \times \text{ARO} = 95.000\,€ \times 0.033 = 3.135\,€$$

Dati Rilevanti

Parametro	Formulario	Calcolo	Valore
AV (Asset Value)			100.000€
EF (Exposure Factor)			95%
ARO (Annualized Rate of Occurrence)	$\frac{1}{30\text{ anni}}$		0.033
SLE (Single Loss Expectancy)	AV × EF	100.000 € × 95%	95.000€
ALE (Annualized Loss Expectancy)	SLE × ARO	95.000 € × 0.033	3.135€

3.3 *Incendio sull'asset «Edificio Primario»*

- **AV (Asset Value):** valore totale dell'asset, che per l'asset edificio primario è pari a 350.000€.
- **EF (Exposure Factor):** percentuale di perdita dell'asset in caso di disastro, che per la coppia edificio primario/incendio è pari al 60%.
- **SLE (Single Loss Expectancy):** l'aspettativa di perdita singola, AV ∗ EF

$$\text{SLE} = 350.000\,€ \times 60\% = 210.000\,€$$

- **ARO (Annualized Rate of Occurrence):** il numero di volte che un evento si verifica in un anno, che per l'evento «Incendio» è 1 volta ogni 20 anni, che equivale a 0.05 volte/anno.
- **ALE (Annualized Loss Expectancy):** l'aspettativa di perdita annualizzata, SLE ∗ ARO

$$\text{ALE} = \text{SLE} \times \text{ARO} = 210.000\,€ \times 0.05 = 10.500\,€$$

Dati Rilevanti

Parametro	Formulario	Calcolo	Valore
AV (Asset Value)			350.000€
EF (Exposure Factor)			60%
ARO (Annualized Rate of Occurrence)	$\frac{1}{20\text{ anni}}$		0.05
SLE (Single Loss Expectancy)	AV × EF	350.000 € × 60%	210.000€
ALE (Annualized Loss Expectancy)	SLE × ARO	210.000 € × 0.05	10.500€

3.4 *Incendio sull'asset «Edificio Secondario»*

- **AV (Asset Value):** valore totale dell'asset, che per l'asset edificio secondario è pari a 150.000€.
- **EF (Exposure Factor):** percentuale di perdita dell'asset in caso di disastro, che per la coppia edificio secondario/incendio è pari al 50%.
- **SLE (Single Loss Expectancy):** l'aspettativa di perdita singola, AV ∗ EF

$$\text{SLE} = 150.000\,€ \times 50\% = 75.000\,€$$

- **ARO (Annualized Rate of Occurrence):** il numero di volte che un evento si verifica in un anno, che per l'evento «Incendio» è 1 volta ogni 20 anni, che equivale a 0.05 volte/anno.
- **ALE (Annualized Loss Expectancy):** l'aspettativa di perdita annualizzata, SLE ∗ ARO

$$\text{ALE} = \text{SLE} \times \text{ARO} = 75.000\,€ \times 0.05 = 3.750\,€$$

Dati Rilevanti

Parametro	Formulario	Calcolo	Valore
AV (Asset Value)			150.000€
EF (Exposure Factor)			50%
ARO (Annualized Rate of Occurrence)	$\frac{1}{20\text{ anni}}$		0.05
SLE (Single Loss Expectancy)	AV × EF	150.000 € × 50%	75.000€
ALE (Annualized Loss Expectancy)	SLE × ARO	75.000 € × 0.05	3.750€

3.5 *Inondazione sull'asset «Edificio Primario»*

- **AV (Asset Value):** valore totale dell'asset, che per l'asset edificio primario è pari a 350.000€.
- **EF (Exposure Factor):** percentuale di perdita dell'asset in caso di disastro, che per la coppia edificio primario/inondazione è pari al 55%.
- **SLE (Single Loss Expectancy):** l'aspettativa di perdita singola, AV ∗ EF

$$\text{SLE} = 350.000\,€ \times 55\% = 192.500\,€$$

- **ARO (Annualized Rate of Occurrence):** il numero di volte che un evento si verifica in un anno, che per l'evento «Inondazione» è 1 volta ogni 50 anni, che equivale a 0.02 volte/anno.
- **ALE (Annualized Loss Expectancy):** l'aspettativa di perdita annualizzata, SLE ∗ ARO

$$\text{ALE} = \text{SLE} \times \text{ARO} = 192.500\,€ \times 0.02 = 3.850\,€$$

Dati Rilevanti

Parametro	Formulario	Calcolo	Valore
AV (Asset Value)			350.000€
EF (Exposure Factor)			55%
ARO (Annualized Rate of Occurrence)	$\frac{1}{50\text{ anni}}$		0.02
SLE (Single Loss Expectancy)	AV × EF	350.000 € × 55%	192.500€
ALE (Annualized Loss Expectancy)	SLE × ARO	192.500 € × 0.02	3.850€

3.6 *Terremoto sull'asset «Edificio Primario»*

- **AV (Asset Value):** valore totale dell'asset, che per l'asset edificio primario è pari a 350.000€.
- **EF (Exposure Factor):** percentuale di perdita dell'asset in caso di disastro, che per la coppia edificio primario/terremoto è pari all'80%.
- **SLE (Single Loss Expectancy):** l'aspettativa di perdita singola, AV ∗ EF

$$\text{SLE} = 350.000\,€ \times 80\% = 280.000\,€$$

- **ARO (Annualized Rate of Occurrence):** il numero di volte che un evento si verifica in un anno, che per l'evento «Terremoto» è 1 volta ogni 30 anni, che equivale a 0.033 volte/anno.
- **ALE (Annualized Loss Expectancy):** l'aspettativa di perdita annualizzata, SLE ∗ ARO

$$\text{ALE} = \text{SLE} \times \text{ARO} = 280.000\,€ \times 0.033 = 9.240\,€$$

Dati Rilevanti

Parametro	Formulario	Calcolo	Valore
AV (Asset Value)			350.000€
EF (Exposure Factor)			80%
ARO (Annualized Rate of Occurrence)	$\frac{1}{30\text{ anni}}$		0.033
SLE (Single Loss Expectancy)	AV × EF	350.000 € × 80%	280.000€
ALE (Annualized Loss Expectancy)	SLE × ARO	280.000 € × 0.033	9.240€

4 CONCLUSIONI

Il Business Continuity Plan (BCP) e il Disaster Recovery Plan (DRP) sono strumenti fondamentali per assicurare la resilienza e la capacità di ripresa delle aziende di fronte a eventi catastrofici come terremoti, inondazioni o incendi. Implementando piani solidi, le aziende possono minimizzare l'interruzione delle operazioni, proteggere i dati cruciali e ridurre i tempi di inattività.

Vantaggi della pianificazione

- **Minimizzazione delle interruzioni:** riduzione al minimo dell'interruzione delle operazioni aziendali durante eventi catastrofici.
- **Protezione dei dati:** salvaguardia dei dati cruciali per garantire la continuità delle operazioni.
- **Riduzione dei tempi di inattività:** implementazione di misure per riprendere le operazioni nel minor tempo possibile.

Processo di sviluppo del BCP e DRP

- **Valutazione degli asset e delle minacce:** comprendere dettagliatamente gli asset aziendali e le potenziali minacce.
- **Identificazione delle risorse critiche:** focalizzare le misure di protezione sugli elementi più vulnerabili e di maggiore valore.
- **Formazione e consapevolezza:** preparazione del personale per reagire rapidamente ed efficientemente durante un'emergenza.

Tecnologie avanzate e collaborazione

- **Tecnologie di monitoraggio e protezione:** utilizzo di sistemi di backup dati in tempo reale, infrastrutture cloud e soluzioni di sicurezza informatica.
- **Collaborazione esterna:** condivisione di risorse e informazioni con enti pubblici e altre organizzazioni per rafforzare la capacità di risposta.

Benefici a lungo termine

- **Vantaggio competitivo:** la resilienza aziendale diventa un differenziatore in un mercato instabile e imprevedibile.
- **Sostenibilità:** promozione della sostenibilità a lungo termine dell'azienda.
- **Proattività nella gestione del rischio:** preservazione del valore aziendale e costruzione di un futuro più sicuro e stabile.

Importanza della preparazione continua

- **Aggiornamento regolare dei piani:** revisione e aggiornamento continuo del BCP e DRP per affrontare le nuove sfide e minacce emergenti.
- **Investimento in formazione:** formazione continua del personale per garantire una risposta efficace alle emergenze.

In conclusione, l'integrazione di un Business Continuity Plan e di un Disaster Recovery Plan ben strutturati protegge gli interessi immediati dell'azienda e promuove la sua sostenibilità a lungo termine. Una preparazione adeguata non solo salvaguarda le risorse fisiche e digitali, ma mantiene anche la fiducia dei clienti e delle parti interessate, garantendo la continuità delle attività aziendali e la stabilità a lungo termine.

5 TABELLA RIASSUNTIVA

Caso Studio	Parametro	Formulario	Calcolo	Valore
Inondazione Edificio Secondario	AV			150.000€
	EF			40%
	ARO	$\frac{1}{50 \text{ anni}}$		0.02
	SLE	AV × EF	150.000 € × 40%	60.000€
	ALE	SLE × ARO	60.000 € × 0.02	1.200€
Terremoto Datacenter	AV			100.000€
	EF			95%
	ARO	$\frac{1}{30 \text{ anni}}$		0.033
	SLE	AV × EF	100.000 € × 95%	95.000€
	ALE	SLE × ARO	95.000 € × 0.033	3.135€
Incendio Edificio Primario	AV			350.000€
	EF			60%
	ARO	$\frac{1}{20 \text{ anni}}$		0.05
	SLE	AV × EF	350.000 € × 60%	210.000€
	ALE	SLE × ARO	210.000 € × 0.05	10.500€
Incendio Edificio Secondario	AV			150.000€
	EF			50%
	ARO	$\frac{1}{20 \text{ anni}}$		0.05
	SLE	AV × EF	150.000 € × 50%	75.000€
	ALE	SLE × ARO	75.000 € × 0.05	3.750€
Inondazione sull'asset «Edificio Primario»	AV			350.000€
	EF			55%
	ARO	$\frac{1}{50 \text{ anni}}$		0.02
	SLE	AV × EF	350.000 € × 55%	192.500€
	ALE	SLE × ARO	192.500 € × 0.02	3.850€
Terremoto Edificio Primario	AV			350.000€
	EF			80%
	ARO	$\frac{1}{30 \text{ anni}}$		0.033
	SLE	AV × EF	350.000 € × 80%	280.000€
	ALE	SLE × ARO	280.000 € × 0.033	9.240€