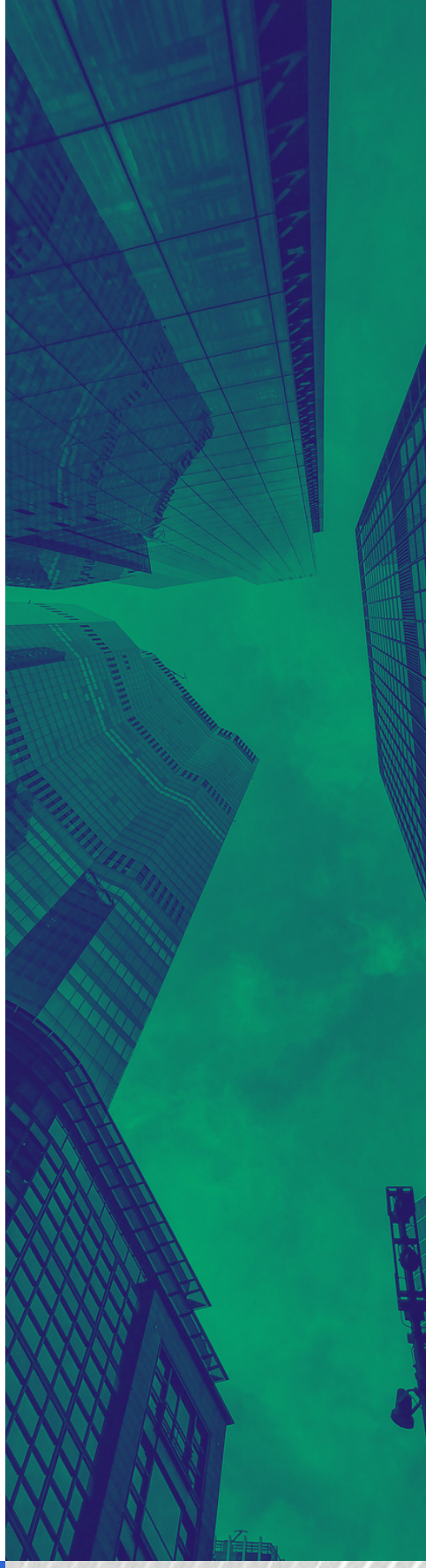
19 MARZO 2024

ASBUG

PC SELL & REPAIR

S9L2 – CS0124



Presented by

BENVENUTI LUIGI
PERTICAROLI FRANCESCO
DI GANGI MANUEL
FICETTI FRANCESCO
DI LIEGGHIO MICHAEL
MARASCA ALESSANDRO
FALCONI BRUNO

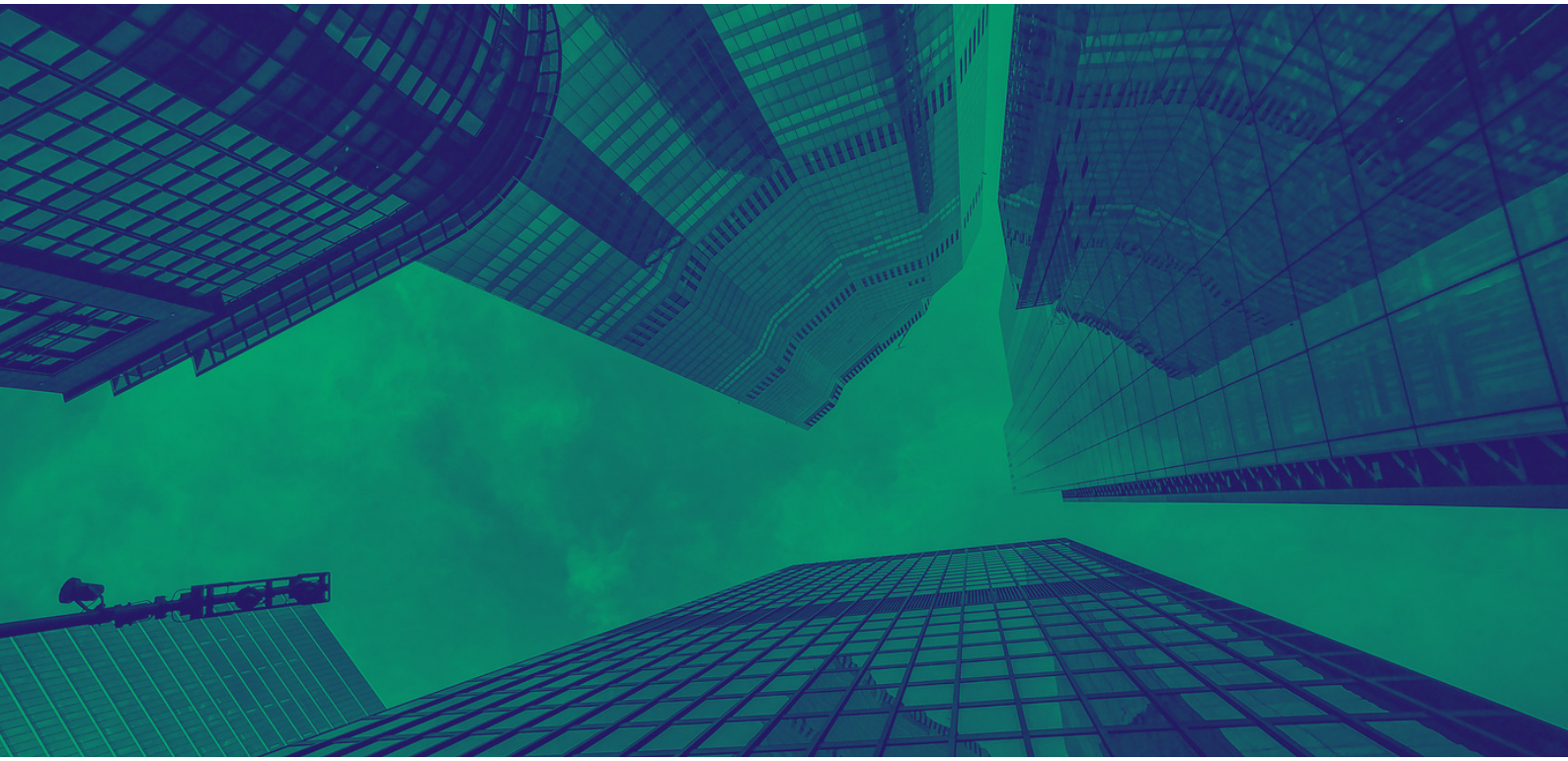
Presented to

FABIANA TARLI

ASBUG

ITALY

INDICE



BCP - BUSINESS PLAN

ASBUG

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»

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%

Business Continuity Plan - ASBUG

INTRODUZIONE

L'azienda **ASBUG** riconosce l'importanza di garantire la continuità operativa e la ripresa delle attività in caso di eventi disruptivi. Questo piano definisce le strategie e le procedure da seguire per mitigare i rischi e ripristinare le operazioni critiche in tempi brevi.

ANALISI DEI RISCHI

Identificazione dei rischi potenziali:

- Guasti hardware o software
- Attacchi informatici
- Disastri naturali (terremoti, incendi, allagamenti)
- Interruzioni dei servizi di fornitura energetica

PIANIFICAZIONE DELLA CONTINUITÀ OPERATIVA

3.1. Ruoli e Responsabilità:

Il responsabile della business continuity coordinerà tutte le attività legate alla continuità operativa.

Il team di risposta agli incidenti sarà responsabile del monitoraggio e della gestione degli eventi di emergenza.

3.2. Pianificazione delle Risorse:

Saranno identificati e documentati tutti i sistemi critici e le risorse necessarie per il loro ripristino.

Saranno stipulati accordi con fornitori di servizi di backup e ripristino, nonché con fornitori di servizi di emergenza e di recupero di disastri.

PREVENZIONE E MITIGAZIONE DEI RISCHI

4.1. Backup e Archiviazione dei Dati:

I dati critici saranno regolarmente e automaticamente salvati su sistemi di backup esterni e sicuri.

Saranno eseguiti test periodici per garantire l'integrità dei backup.

4.2. Sicurezza Informatica:

Saranno implementate misure di sicurezza informatica avanzate per proteggere i sistemi e i dati dall'accesso non autorizzato e dagli attacchi informatici.

RISPOSTA AGLI EVENTI

5.1. Monitoraggio Continuo:

Sarà attivato un sistema di monitoraggio continuo per rilevare tempestivamente eventuali anomalie o segnali di problemi.

5.2. Attivazione del Piano:
In caso di emergenza, il responsabile della business continuity attiverà il piano e coordinerà il team di risposta agli incidenti.

RIPRISTINO DELLE OPERAZIONI
6.1. Priorità di Ripristino:
Saranno definiti i tempi massimi accettabili per il ripristino dei sistemi e delle operazioni critiche.
Saranno identificati e stabiliti i processi di ripristino prioritari per minimizzare l'impatto sulle attività aziendali.
6.2. Test del Piano:
Saranno condotti regolarmente test di ripristino per valutare l'efficacia del piano e apportare eventuali miglioramenti.
Revisione e Aggiornamento del Piano
Il piano di business continuity sarà periodicamente rivisto e aggiornato per garantire la sua efficacia e la sua adattabilità ai cambiamenti nell'ambiente operativo e nei rischi identificati.
Contatti di Emergenza
Saranno forniti i contatti di emergenza del team di risposta agli incidenti e dei fornitori di servizi critici.

APPROVAZIONE E DISTRIBUZIONE
Il presente piano sarà approvato dal management aziendale e distribuito a tutti i dipendenti coinvolti nella sua implementazione e attuazione.

COSA FACCIAMO?

DIPARTIMENTO VENDITE COMPONENTISTICA

DIPARTIMENTO ASSISTENZA COMPUTER

RIPARA IL TUO PC

$100 / H

Pronto in 24 ore, soddisfatto o rimborsato

COMPRA IL TUO PC

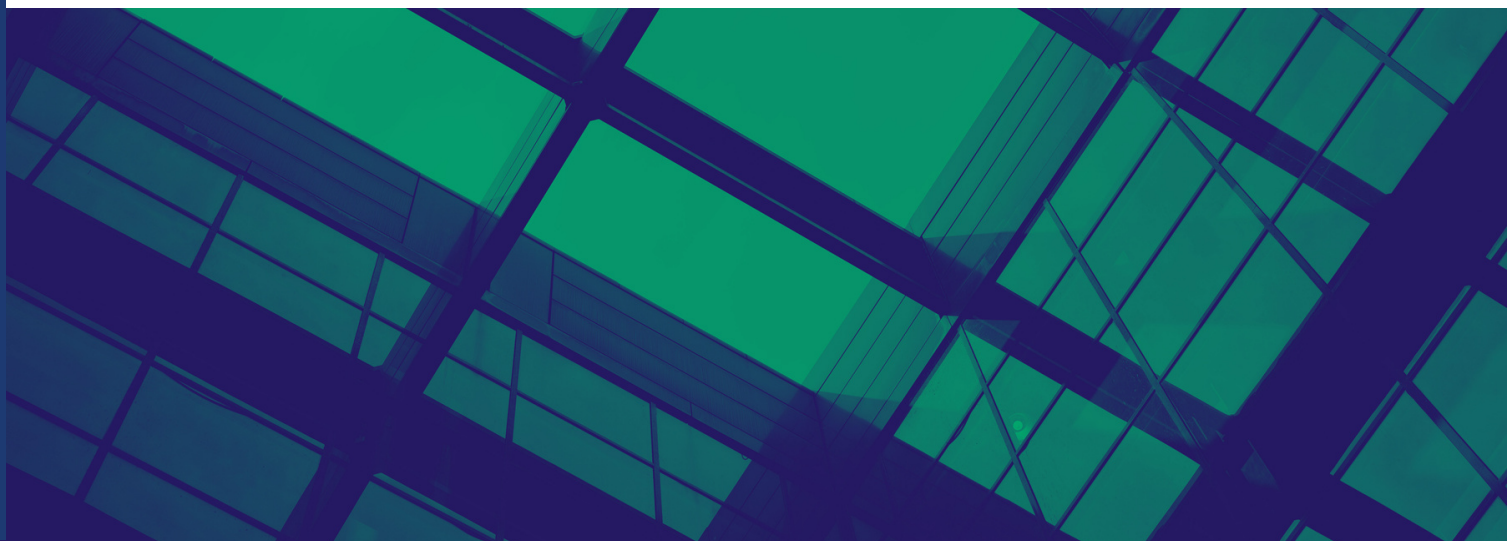
Acquista da noi il tuo PC personalizzato!
Assemblaggio incluso nel prezzo

LOGISTICA

CORE BUSINESS

La nostra azienda basa il suo know-how sull'assistenza per PC ad alta performatività.
Inoltre, fornisce un servizio di vendita diretta di componentistica.
I nostri **edifici** sono:

Edificio A - Dipartimento Amministrativo
Edificio B - Data Center
Edificio C - Dipartimento Operativo



EDIFICIO A	EDIFICIO B	EDIFICIO C
Amministrazione	Data Center	Reparto riparazioni
Segreteria		Assemblaggio
Punto Vendita		Logistica

IDENTIFICAZIONE PRIORITA’

1. **Il reparto amministrativo e di segreteria** deve garantire operatività continua per rispondere in maniera immediata alle richieste dei clienti e per fornire informazioni relative ai servizi erogati.
2. **Il reparto assemblaggio e assistenza** fornisce esecutività costante per soddisfare le richieste dei clienti nelle tempistiche stabilite.
3. **Il punto vendita** non rappresenta il **core business** dell’azienda; un eventuale indisponibilità temporanea avrebbe dunque un impatto minore.

BENVENUTI LUIGI	FRANCESCO FICETTI	MANUEL DI GANGI	BRUNO FALCONI
Amministratore unico	Responsabile IT	Responsabile Cyber Sicurezza	Responsabile della sicurezza fisica

FRANCESCO PERTICAROLI	ALESSANDRO MARASCA	MICHAEL DI LIEGGHIO
Responsabile del Team Legale	Responsabile risorse umane	Responsabile Servizio Assistenza

BUSINESS IMPACT ANALYSIS

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:

DISASTRI NATURALI	DISASTRI CAUSATI DALL'UOMO
Terremoti	Atti di terrorismo
Inondazioni	Esplosioni
Temporali	Interruzioni di corrente
Maremoti	Guasti infrastrutturali o di rete

MAXIMUM TOLERABLE DOWNTIME (MTD): 1 GIORNO

RECOVERY TIME OBJECTIVE (RTO): 3 ORE

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.

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

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.

Da un punto di vista quantitativo: si assegna ad ogni asset quello che viene chiamato «**Exposure Factor** » (EF), misurato come la percentuale di asset che verrebbe impattato a seguito del verificarsi di un determinato evento, e si introduce il concetto di «**Single Loss Expectancy**» (SLE), che ci dà una misura monetaria della perdita che si subirebbe al verificarsi dell'evento, calcolato come il prodotto tra il **valore dell'asset** (AV) e la percentuale impattata in caso di evento (EF) :

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

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

```
Innondazione sull'assets <<edificio secondario>>
SLE = AV x EF = 150.000€ x 0,40 = 60.000
ALE = SLE x ARO = 60.000€ x 0.02 = 1200€/anno

Terremoto sull'assets <<datacenter>>
SLE = AV x EF = 100.000€ x 0.95 = 95.000
SLE = AV x EF = 95.000€ x 0.03 = 2.850€/anno

Incendio sull'assets <<edificio primario>>
SLE = AV x EF = 350.000€ x 0.60 = 210.000
SLE = AV x EF = 210.000€ x 0.05 = 10.500€/anno

Incendio sull'assets <<edificio secondario>>
SLE = AV x EF = 150.000€ x 0.50 = 75.000€
ALE = SLE x ARO = 75.000€ x 0.05 = 3.750€/anno

Innondazione sull'assets <<edificio primario>>
SLE = AV x EF = 350.000€ x 0.55 = 192.500€
ALE = SLE x ARO = 192.500€ x 0.02 = 3.810€/anno

Terremoto sull'assets <<edificio primario>>
SLE = AV x EF = 350.000€ x 0.80 = 280.000€
ALE = SLE x ARO = 280.000€ x 0.03 = 8.400€/anno
```

BUSINESS CONTINUITY PLANNING

La fase del continuity planning ha invece lo scopo di sviluppare e di Implementare una strategia per la riduzione dell'impatto dei rischi sugli asset protetti.

Sviluppo della strategia:
se nella BIA si identificano rischi ed asset prioritari, nella fase di sviluppo della 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.

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.

Ecco le misure di sicurezza predisposte all'interno dell'azienda:

- Controllo degli accessi: ogni dipendente dispone di un badge personale, questo permette di tener traccia degli utente e dei loro privilegi di accesso.
- Addetti alla sicurezza;
- Sistema di video sorveglianza;
- Piani di evacuazione in caso di incendio o calamità naturale;
- Impianto antincendio;
- Gruppi di continuità per gli asset critici;
- Impianto di raffreddamento per i sistemi presenti nel data center;
- Backup quotidiani per assicurare la persistenza dei dati e garantendone la disponibilità in caso di ripristino in caso di perdita o danneggiamento.

PER L'EDIFICIO PRIMARIO:

Probabilità di Terremoto:

ARO (Annual Rate of Occurrence) = 1/30 = 0.0333

Exposure Factor al Terremoto:

EF (Exposure Factor) = 80%

Perdita Attesa per il Terremoto sull'Edificio Primario:

Loss = Valore dell'Edificio Primario * EF = 350,000 * 0.8 = 280,000 euro

Probabilità di Incendio:

ARO = 1/20 = 0.05

Exposure Factor all'Incendio:

EF = 60%

Perdita Attesa per l'Incendio sull'Edificio Primario:

Loss = 350,000 * 0.6 = 210,000 euro

Probabilità di Inondazione:

ARO = 1/50 = 0.02

Exposure Factor all'Inondazione:

EF = 55%

Perdita Attesa per l'Inondazione sull'Edificio Primario:

Loss = 350,000 * 0.55 = 192,500 euro

Perdita Totale Annua per l'Edificio Primario:

Perdita Terremoto + Perdita Incendio + Perdita Inondazione = 280,000 + 210,000 + 192,500 = **682,500 euro**

PER L'EDIFICIO SECONDARIO:

Probabilità di Terremoto:

ARO = 1/30 = 0.0333

Exposure Factor al Terremoto:

EF = 80%

Perdita Attesa per il Terremoto sull'Edificio Secondario:

Loss = Valore dell'Edificio Secondario * EF = 150,000 * 0.8 = 120,000 euro

Probabilità di Incendio:

ARO = 1/20 = 0.05

Exposure Factor all'Incendio:

EF = 50%

Perdita Attesa per l'Incendio sull'Edificio Secondario:

Loss = 150,000 * 0.5 = 75,000 euro

Probabilità di Inondazione:

ARO = 1/50 = 0.02

Exposure Factor all'Inondazione:

EF = 40%

Perdita Attesa per l'Inondazione sull'Edificio Secondario:

Loss = 150,000 * 0.4 = 60,000 euro

Perdita Totale Annua per l'Edificio Secondario:

Perdita Terremoto + Perdita Incendio + Perdita Inondazione = 120,000 + 75,000 + 60,000 = **255,000 euro**

PER IL DATACENTER:

Probabilità di Terremoto:

ARO = 1/30 = 0.0333

Exposure Factor al Terremoto:

EF = 95%

Perdita Attesa per il Terremoto sul Datacenter:

Loss = Valore del Datacenter * EF = 100,000 * 0.95 = 95,000 euro

Probabilità di Incendio:

ARO = 1/20 = 0.05

Exposure Factor all'Incendio:

EF = 60%

Perdita Attesa per l'Incendio sul Datacenter:

Loss = 100,000 * 0.6 = 60,000 euro

Probabilità di Inondazione:

ARO = 1/50 = 0.02

Exposure Factor all'Inondazione:

EF = 35%

Perdita Attesa per l'Inondazione sul Datacenter:

Loss = 100,000 * 0.35 = 35,000 euro

Perdita Totale Annua per il Datacenter:

Perdita Terremoto + Perdita Incendio + Perdita Inondazione = 95,000 + 60,000 + 35,000 = **190,000 euro**

Perdite annuali previste per ciascun asset:

Edificio Primario: 682,500 euro
Edificio Secondario: 255,000 euro
Datacenter: 190,000 euro

DISASTER RECOVERY PLAN

Il **disaster recovery planning** include i controlli tecnici da implementare per la riduzione del rischio e per il recupero dei servizi a valle di un evento catastrofico.

Nello sviluppo di un piano di disaster recovery, i seguenti documenti devono essere presenti:

• **Executive summary**, un documento che andrà al management, al cui interno sarà presentata una vista globale sul piano di disaster recovery;
• **Un documento tecnico per il personale IT** responsabile dell'implementazione e della manutenzione dei sistemi;
• **Un piano d'azione le persone ingaggiate** nel piano di disaster recovery;
• **Copie complete del piano** per i responsabili primari dell'implementazione e attuazione del piano.

PROTEZIONE RISCHI E IMPLEMENTAZIONI

1. **RAID 6**, principio di archiviazione che richiede un minimo di 4 dischi e tollera simultaneamente il guasto di due dischi senza perdita di dati;
2. **Server principale in cluster**, coppia di server che si comportano come se fosse uno solo, in caso di guasto del server principale, il secondario subentra automaticamente per mantenere l'operatività senza interruzioni;
3. **Generatori di emergenza**, pronti ad intervenire in caso di mancanza della fornitura elettrica;
4. I**mplementazione della tecnica di backup '3-2-1'**: devono essere effettuate 3 copie di backup, di cui 2 salvate nei server locali (possibilmente in due luoghi geograficamente separati), ed una salvata in cloud;
5. **Strategia di backup**: un full backup viene effettuato la domenica ed ulteriori backup incrementali durante la settimana, ritenzione di 1 mese;
6. **Replica dei server/NAS principali:** ogni sera, il server e i NAS principali vengono replicati nel nostro data center di emergenza, in grado di fornire i servizi necessari al funzionamento base dell'azienda.

GRAZIE

BENVENUTI LUIGI

PERTICAROLI FRANCESCO

DI GANGI MANUEL

FICETTI FRANCESCO

DI LIEGGHIO MICHAEL

MARASCA ALESSANDRO

FALCONI BRUNO