Project Name	Business continuity and disaster recovery	**Reporting Period**
Project Owner	USR robotics	19/03/2024 - 19/03/2025
Prepared by	Noi	

HIGHLIGHTS

- business continuity
- disaster recovery

L’azienda

L’azienda si occupa di internet service provider (ISP)

Le aziende Internet provider offrono servizi di connettività Internet agli utenti finali, sia a livello domestico che aziendale. Questi servizi includono l'accesso a Internet ad alta velocità tramite tecnologie come la banda larga, la fibra ottica, il DSL, il cavo, il wireless e altri. Di

solito, gli ISP offrono anche servizi aggiuntivi come l'hosting web, l'email, la telefonia VoIP e altro ancora.

Ecco alcuni dei principali aspetti delle aziende Internet provider:

Accesso a Internet: Gli ISP forniscono agli utenti finali accesso alla rete Internet. Questo può includere l'installazione di linee fisiche, come cavi in fibra ottica o rame, o l'accesso wireless tramite tecnologie come il Wi-Fi o il 4G/5G.

Piani tariffari: Gli ISP offrono una varietà di piani tariffari che differiscono per velocità di connessione, limiti di dati e altri servizi inclusi. Gli utenti possono scegliere il piano che meglio si adatta alle loro esigenze e al loro budget.

Servizi aggiuntivi: Oltre alla connettività Internet, molti ISP offrono servizi aggiuntivi come l'hosting web, l'email, la telefonia VoIP, la televisione via Internet (IPTV) e altro ancora. Questi servizi possono essere offerti come pacchetti integrati o come opzioni aggiuntive.

Assistenza clienti: Gli ISP forniscono assistenza tecnica e supporto clienti per risolvere eventuali problemi di connettività o altri problemi che gli utenti possono incontrare. Questo può essere fornito tramite telefono, chat online o altri mezzi di comunicazione.

Infrastruttura di rete: Gli ISP devono gestire e mantenere una robusta infrastruttura di rete per garantire una connettività Internet affidabile e di alta qualità. Questa infrastruttura può includere server, router, switch, linee di trasmissione e altro ancora.

Conformità normativa: Gli ISP devono conformarsi alle normative e alle leggi locali e nazionali relative alla privacy dei dati, alla sicurezza delle reti, alla neutralità della rete e ad altri aspetti della fornitura di servizi Internet.

In sintesi, le aziende Internet provider svolgono un ruolo fondamentale nel fornire accesso a Internet agli utenti finali e offrono una gamma di servizi e soluzioni per soddisfare le esigenze di connettività della clientela.

La struttura

2 sedi operative: una principale, una di cold site(qual'ora la principale sia compromessa)

1 sala server privata (con annesso backup)

Disaster Recovery

Un piano di disaster recovery (DRP) è un documento formale che definisce le procedure e le strategie per ripristinare le operazioni IT e di business dopo un evento catastrofico o un'interruzione significativa. Ecco una guida generale su cosa includere in un piano di disaster recovery:

Scopo e obiettivi: Definire chiaramente lo scopo del piano di disaster recovery e gli obiettivi che si intendono raggiungere:

Nel nostro caso specifico, la continuità del servizio

Situazione attuale: Fornire una panoramica della situazione attuale, inclusi gli asset IT critici, i processi aziendali e le vulnerabilità esistenti.

attualmente vi sono 7 risorse:

un rappresentate dei dirigenti

un team legale

un esperto contabile/amministrativo

un esperto HR

un esperto IT

un esperto in Cybersecurity

un esperto in sicurezza fisica

Analisi dei rischi: Identificare e valutare i potenziali rischi e minacce che potrebbero causare interruzioni alle operazioni, come disastri naturali, attacchi informatici, errori umani, guasti hardware.

esempio: mancanza energia, terremoto, incendio, inondazioni, attacchi hacker, attacchi terroristici,

Procedure di backup e ripristino dei dati: Definire le procedure per eseguire backup regolari dei dati critici e ripristinarli in caso di perdita o danneggiamento. Specificare i tempi di backup, la frequenza e i metodi di archiviazione.

ci appoggiamo al servizio di cloud di amazon, utilizzando server di backup essendo un sistema incrementale è in continuo aggiornamento

Procedure di ripristino dei sistemi: Dettagliare come ripristinare l'infrastruttura IT, inclusi server, reti, applicazioni e database, dopo un'interruzione. Questo può includere l'uso di sistemi di mirroring, snapshot, virtualizzazione e altri strumenti.

utilizziamo un sistema di virtualizzazione per avere sempre accessibilità ai sistemi

Pianificazione della continuità operativa: Definire le procedure per mantenere le operazioni critiche durante un'interruzione. Questo potrebbe includere l'attivazione di siti di continuità operativa, l'uso di sistemi di backup temporanei e la pianificazione delle risorse umane e materiali.

• seconda sede qualora la principale fosse inagibile

Procedure di comunicazione: Stabilire un piano di comunicazione per informare il personale, i clienti, i fornitori e altre parti interessate durante un'interruzione. Chiarezza e tempestività sono cruciali per gestire efficacemente una crisi.

• gruppo telegram (privato) per i dipendenti interni, status dei server sulla pagina web.

Test e manutenzione: Programmare test regolari del piano di disaster recovery per garantire che sia efficace e aggiornato. Anche la manutenzione continua è importante per adattarsi ai cambiamenti nell'infrastruttura IT e nelle esigenze aziendali.

Ruoli e responsabilità: Assegnare chiaramente ruoli e responsabilità a membri specifici del team per garantire un'implementazione efficace del piano durante un'emergenza.

• il rappresentate dei dirigenti: assegna ruoli e decide il futuro operativo aziendale;

• il team legale: verifiche cause in atto;

• il esperto contabile/amministrativo: controllo sul bilancio;

• il responsabile HR: contratti e colloqui per verificare il wellness;

• l'esperto IT : controllo dell'operatività;

• l'esperto in Cybersecurity: controlla attacchi lato server;

• l' esperto in sicurezza fisica: controllo all'ingresso.

Formazione e sensibilizzazione: Assicurarsi che il personale sia adeguatamente formato sulle procedure di disaster recovery e consapevole dei propri ruoli durante un'interruzione.

• sono stati programmati sia corsi per la formazione del personale sia corsi sulla sicurezza sul lavoro che aggiornamento sulle mansioni.

Revisione e miglioramento: Programmare regolarmente revisioni del piano di disaster recovery per identificare aree di miglioramento e aggiornare di conseguenza il documento.

• revisioni in base al cambio di organigramma:

La business continuity

La business continuity (continuità operativa) è un concetto chiave nell'ambito della gestione aziendale che si riferisce alla capacità di un'organizzazione di mantenere le sue operazioni essenziali durante e dopo un'interruzione imprevista o un evento catastrofico. Questo concetto si concentra sulla pianificazione e sull'implementazione di misure preventive e di ripristino per garantire che l'azienda possa continuare a funzionare anche in situazioni di emergenza.

Ecco alcuni aspetti cruciali della business continuity:

Identificazione delle attività critiche: È fondamentale per un'organizzazione identificare le attività, i processi e i servizi che sono essenziali per il funzionamento quotidiano e il raggiungimento degli obiettivi aziendali. Queste possono includere servizi clienti, produzione, comunicazioni, gestione finanziaria, ecc.

Analisi dei rischi: Le organizzazioni devono valutare e comprendere i rischi potenziali che potrebbero influenzare le loro operazioni. Questi rischi possono derivare da una vasta gamma di fonti, tra cui eventi naturali, incidenti tecnologici, minacce informatiche, interruzioni dei fornitori e altro ancora.

Pianificazione e preparazione: Basandosi sull'analisi dei rischi, le organizzazioni sviluppano piani e strategie per affrontare e mitigare gli impatti potenziali di tali rischi. Ciò può includere l'implementazione di misure preventive, la creazione di procedure di risposta agli incidenti e l'allocazione di risorse per affrontare situazioni di emergenza.

Continuità delle operazioni: Durante un'interruzione, è fondamentale che l'organizzazione sia in grado di mantenere le sue operazioni critiche il più possibile. Ciò può richiedere l'attivazione di piani di continuità operativa che consentano alle attività essenziali di continuare nonostante l'evento avverso.

Ripristino e recupero: Dopo che l'emergenza è stata gestita, l'organizzazione deve concentrarsi sul ripristino delle operazioni normali il più rapidamente possibile. Ciò può includere il ripristino dei sistemi IT, la ricostruzione di infrastrutture danneggiate e altre azioni volte a riportare l'azienda alla normalità.

Test e esercitazioni: È vitale testare regolarmente i piani di business continuity per garantire che siano efficaci e aggiornati. Gli esercizi di simulazione consentono all'organizzazione di valutare la propria preparazione e identificare eventuali aree di miglioramento.

Comunicazione e coinvolgimento degli stakeholder: Durante un'interruzione, la comunicazione chiara e tempestiva con il personale, i clienti, i fornitori e altre parti interessate è essenziale per gestire l'emergenza in modo efficace e per mantenere la fiducia nelle capacità dell'organizzazione.

In sintesi, la business continuity è un elemento cruciale della gestione aziendale che mira a garantire la resilienza e la continuità delle operazioni di un'organizzazione anche in situazioni critiche o di emergenza. Un'adeguata pianificazione e preparazione possono fare la differenza nel limitare gli impatti negativi di eventi imprevisti e consentire all'azienda di riprendersi rapidamente e con successo

La valutazione dei rischi

Calcoliamo adesso 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»

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%

1) Inondazione nell edificio secondario
Con il supporto dei dati in tabella, SLE = AV x EF, dove:
AV: asset value, che per l'asset edificio secondario è pari a 150.000€
EF: exposure factor, che per la coppia edificio secondario/inondazione è pari al 40%.
Di conseguenza SLE = 150.000€ x 0,40 = 60.000€
Quindi, ogni volta che un'inondazione si verifica, l'impatto sulla compagnia per l'asset «edificio secondario» è di 60.000€.
Per ricavare la perdita annuale, dobbiamo moltiplicare il valore appena trovato per il tasso di occorrenza annuale dell'evento. Dalla tabella in traccia, vediamo che l'indice ARO per l'evento «inondazione» è 1 volta ogni 50 anni, che equivale a 0,02 volte.
Di conseguenza, ALE = SLE x ARO = 60.000€ x 0,02 = 1200€. L'impatto sulla compagnia per l'evento incendio sull'asset edificio secondario è di 1200€/anno.

2)Terremoto sul datacenter
SLE = 100.000€ x 0,95 = 95.000€
Ale = 95.000€ x 0,03 = 2850€

3)Incendio nell edificio primario
SLE = 350.000€ x 0,60 = 210.000€
Ale = 210.000€ x 0,05 = 10.500€

4)Incendio nell edificio secondario
SLE = 150.000€ x 0,50 = 75.000€
Ale = 75.000€ x 0,02 = 1500€

5)Inondazione nell edificio primazio
SLE = 350.000€ x 0,55 = 192.500€
Ale = 192.500€ x 0,05 = 9600€

6)Terremoto nell edificio primazio
SLE = 350.000€ x 0,80 = 280.000€
Ale = 280.000€ x 0,03 = 8400€