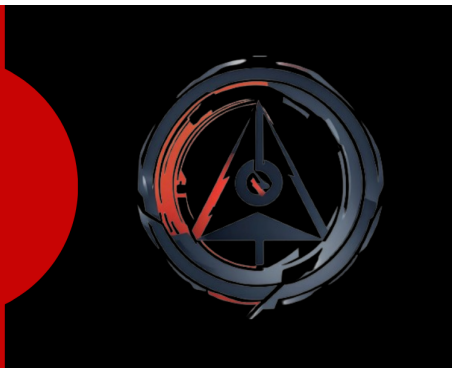
Business Continuity Plan



1. FINALITA' E AMBITO DI APPLICAZIONE – ATTIVITA' DI CUSTOMER SUPPORT

Nell'ambito delle attività di CyberSecureTech, il customer support si distingue per la sua importanza, richiedendo una continuità costante del servizio offerto al cliente. Per garantire questa continuità, la Società ha sviluppato un Piano di Continuità Operativa (BCP) e un Piano di Disaster Recovery (DR). Questi piani contengono procedure specifiche per gestire e superare situazioni di emergenza e disastro che potrebbero ostacolare il normale svolgimento delle attività.

In caso di emergenza o disastro, è fondamentale garantire:

1. Accessibilità delle sedi operative.
2. Disponibilità del personale essenziale per l'erogazione del servizio.
3. Funzionamento dei servizi infrastrutturali.
4. Accesso e conservazione dei dati necessari per svolgere il servizio.
5. Funzionamento del sistema informativo.

Il Piano di Continuità Operativa (BCP) documenta tutte le informazioni e le procedure necessarie per gestire eventi straordinari che possano compromettere le attività ordinarie della Società. All'interno del BCP, vi è una sezione dedicata al Piano di Disaster Recovery (DR), che definisce i possibili disastri e scenari di rischio, identifica i processi critici e le figure di riferimento, sia interne che esterne alla Società, e descrive le modalità di risoluzione dei problemi gravi.

Tutti i dipendenti sono istruiti sulle procedure da seguire in caso di disastro o emergenza, per assicurare la continuità del customer support anche durante eventi critici. Questo documento ha l'obiettivo di delineare le modalità tecnico-organizzative che la Società deve seguire per mantenere operativi i propri servizi entro un tempo prestabilito dopo un disastro o un evento dannoso.

Nel redigere il Piano di Continuità Operativa, la Società ha analizzato e mitigato le cause di rischio, incrementando i livelli di sicurezza delle proprie strutture. Il Piano contiene tutte le informazioni relative all'organizzazione logistica della Società, dalla dichiarazione dell'emergenza al ritorno alla normalità, includendo le metodologie per riconoscere e gestire una situazione di crisi. Questo Piano comprende i processi di

gestione della crisi e del disaster recovery, delineando le procedure per ripristinare le attività e garantire la continuità dei servizi.

Il Piano stabilisce le procedure alternative da adottare in caso di disastro, per garantire l'operatività di CyberSecureTech. Attraverso test periodici, viene verificata l'efficacia delle procedure di ripristino.

Il servizio di customer support offerto dalla nostra Società è classificato come "critico" a causa delle sue implicazioni per i clienti. In caso di mancanza di alcuni elementi essenziali per il suo svolgimento (ad esempio, personale, attrezzature informatiche, servizi di telecomunicazione), risulta impossibile erogarlo, con gravi ripercussioni sulla qualità del servizio.

Il Piano di Continuità Operativa valuta la criticità del servizio e prevede strategie di ripristino come l'utilizzo di un sito alternativo, metodologie e apparecchiature per il backup, nonché la definizione dei ruoli e delle responsabilità delle figure coinvolte. Particolare attenzione è dedicata alla definizione degli scenari di disastro, poiché il mancato riconoscimento tempestivo della gravità della situazione può causare ritardi irreparabili nella dichiarazione di emergenza e nella sua gestione.

Il personale addetto al servizio ha il compito di rilevare le condizioni di emergenza e comunicarle alla struttura aziendale preposta alla gestione delle crisi (Comitato Gestione Crisi), che si attiverà nei tempi e con le modalità previste dal presente Piano.

2. TLC

Gli strumenti di telecomunicazione utilizzati dalla nostra Società includono: PC, telefoni collegati alla rete fissa, telefoni mobili e un collegamento internet con una velocità di 20 mega e 512 K garantiti. La sede principale è dotata di un impianto elettrico in cui i PC, i telefoni fissi e i componenti hardware centralizzati sono alimentati da un gruppo di continuità UPS, che assicura la funzionalità in caso di variazioni o assenza di tensione per circa 30 minuti.

Nella nostra sede, sono presenti complessivamente 8 canali di fonia, suddivisi in 4 collegamenti BRI ISDN da 2 canali ciascuno: due dedicati al supporto delle Stazioni Appaltanti e due al supporto degli Operatori Economici che utilizzano le piattaforme gestite dal customer support. Il tutto è gestito da un sistema centralizzato VOIP con alta affidabilità, grazie a due hardware fisici con le stesse capacità situati in sedi diverse, capaci di sostituirsi reciprocamente.

Gli addetti al customer support dispongono ciascuno di un computer fisso collegato alla rete aziendale. Ogni computer ha accesso alle caselle e-mail dedicate al servizio per ciascun ente/piattaforma, con relativa archiviazione locale.

In caso di evento dannoso, la continuità operativa del servizio è garantita nei seguenti modi:

- Immediatamente dopo il verificarsi di un malfunzionamento nella sede principale:
- Linee telefoniche: gli addetti al customer support utilizzano cellulari di servizio in caso di indisponibilità della rete fissa.
- Linea internet: in caso di indisponibilità del collegamento, gli operatori utilizzano router portatili per connettersi a internet tramite UMTS e continuare a erogare il servizio.
- Computer: nella sede principale sono disponibili PC portatili programmati con i software e gli accessi necessari (es. piattaforme, posta elettronica, software per l'attività di customer support) per garantire l'operatività del servizio in caso di mancanza di corrente elettrica, con un'autonomia di circa 2 ore per PC. Le batterie dei PC portatili vengono verificate settimanalmente e, se necessario, ricaricate.
- Successivamente, trasferendosi nella sede secondaria:
- Linee telefoniche fisse: la sede secondaria è dotata di una propria rete telefonica fissa, sulla quale vengono dirottate le telefonate in entrata di Stazioni Appaltanti e Operatori Economici.
- Linea internet: la sede secondaria dispone di una rete internet da 20 mega, che assicura l'erogazione del servizio da parte degli addetti al customer support.

Inoltre, i router portatili possono essere trasferiti nella sede secondaria, se necessario.

- Pc portatili: PC portatili: in caso di trasferimento nella sede secondaria, gli addetti porteranno con sé i PC portatili sopra descritti, che potranno essere ricaricati alla rete elettrica (se disponibile). Inoltre, avranno a disposizione altri due PC portatili già presenti in loco.

3. SERVIZIO DI ARCHIVIAZIONE E ATTIVITA' DI RECUPERO DATI

Tutti i dati acquisiti durante il servizio di customer support, insieme agli altri dati prodotti o acquisiti dall'azienda, sono archiviati in tempo reale su uno storage dotato di backup automatico e sincronizzazione in cloud. Il salvataggio dei dati viene replicato quotidianamente, in modo automatico, su ulteriori supporti hardware (PC fissi, hard disk USB, storage secondario).

Lo storage principale conserva lo storico dei salvataggi dell'ultima settimana, garantendo il recupero dei dati in caso di perdita accidentale, grazie all'accesso all'ultimo backup effettuato. Inoltre, è attivo uno storage di backup dedicato alla ridondanza dei dati, situato nell'ufficio adiacente alla sede principale. Questo storage secondario è anch'esso sincronizzato al cloud, assicurando un backup automatico e in tempo reale di tutti i dati. In caso di necessità, lo storage secondario può essere trasferito nella sede secondaria, da cui è comunque garantito l'accesso al cloud.

Per i dati archiviati in cloud, il disaster recovery è gestito dai fornitori dei servizi cloud, come specificato nella Parte B del documento. La posta elettronica, sia in entrata che in uscita, è archiviata in cloud e replicata su un hardware con un backup settimanale.

Ogni PC utilizzato dalla Società è dotato di un firewall software. Per aumentare la sicurezza dei dati, è stato installato anche un firewall hardware.

4. TEMPI ENTRO I QUALI I SERVIZI DEVONO ESSERE RECUPERATI (RTO)

L'RTO (Recovery Time Objective) rappresenta il tempo massimo accettabile per ripristinare i servizi di customer support senza causare un disservizio irreparabile in termini di qualità.

Questo tempo è fissato a 60 minuti, considerato il periodo necessario per riattivare le telecomunicazioni e ristabilire l'operatività del servizio.

L'RTO è diviso in diverse fasi per il recupero dell'operatività, anche se parziale, per riuscire a far fronte alle richieste dei clienti:

- In 20 minuti dall'evento distruptive: utilizzo di router portatili per garantire connessione internet e continuare a utilizzare i PC.
- In 40 minuti dall'evento distruptive: raggiungimento della sede secondaria.
- In 60 minuti dall'evento distruptive: ripristino dell'operatività nella sede secondaria.

5. LIVELLI DI RECUPERO NECESSARIO PER OGNI SERVIZIO (RPO)

L'RPO (Recovery Point Objective) è la massima perdita di dati tollerata.

I tipi di dati prodotti e gestiti sono delle seguenti tipologie:

- Telefonate: l'entità delle telefonate, il numero e il contenuto vengono registrate su un calendar condiviso in cloud Microsoft e archiviate automaticamente in tempo reale.
- E-mail: sono archiviate in locale sui singoli PC e in cloud istantaneamente dal loro invio o ricezione. Ogni settimana le e-mail sono salvate su un hardware di back-up.
- Documenti: prodotti e gestiti sono realizzati e archiviati direttamente sulle cartelle di file con back-up automatico sul cloud Google Drive.

6. CONDIZIONI LIMITE CHE PORTANO ALL'ATTUAZIONE DEL PIANO

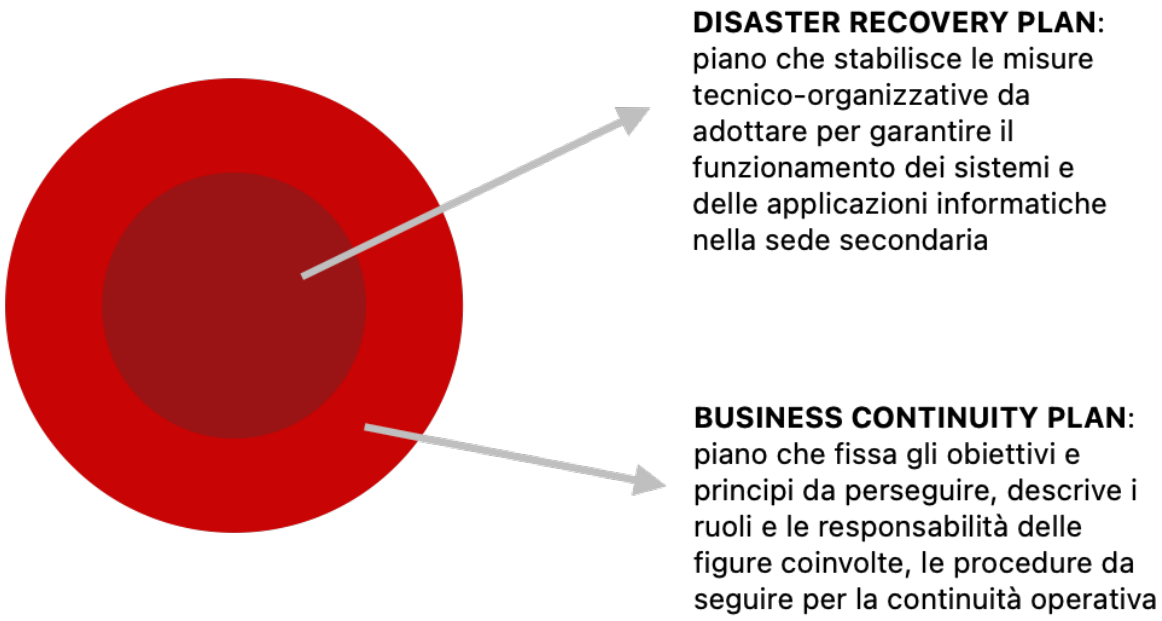
Le condizioni per le quali è necessario ricorrere alla continuità operativa sono:

1. Indisponibilità della sede primaria per eventi naturali, assenza prolungata dell’energia elettrica o della rete internet.
2. Indisponibilità di personale essenziale: Mancanza massiva di personale dovuta, per esempio, a epidemia influenzale o strade bloccate.
3. Perdita documentazione.

7. TABELLA DI CLASSIFICAZIONE DEGLI INCIDENTI

Livello	**Classe Incidente**	**Descrizione**
0	ORDINARIO (non significativo)	L'incidente non ha causato disservizi significativi e l'impatto sull'operatività dell’azienda è trascurabile. L'evento può essere risolto con mezzi di intervento ordinari.
1	SIGNIFICATIVO	Degrado o interruzione di una percentuale minoritaria (< 25%) del servizio, che continua ad essere erogato anche se con modalità rallentata.
2	GRAVE	Degrado o interruzione di una percentuale da media a elevata (26% - 55%) del servizio, che continua ad essere erogato ma provoca gravi disservizi.
3	DISASTROSO	Incidente che causa l'interruzione di una percentuale significativa del servizio (56% - 100%).

Il Piano di Disaster Recovery, parte integrante del BCP, comprende azioni e sistemi per il ripristino delle funzionalità tecnologiche e organizzative dell'azienda. Descrive le misure tecnologiche e logistico-organizzative necessarie per ripristinare sistemi, dati e infrastrutture, garantendo la continuità del servizio di customer support in caso di gravi emergenze che compromettano la normale attività.



1. FINALITÀ E CONTENUTI DEL PIANO DI DISASTER RECOVERY

Il Piano di Disaster Recovery ha la funzione di spiegare nel dettaglio le fasi necessarie per il ripristino delle risorse hardware e software utilizzate per l'erogazione del servizio da parte degli operatori del customer support.

Nel piano di DR vengono dettagliate le procedure operative necessarie per effettuare una corretta valutazione della situazione di emergenza/disastro che impedisce la normale erogazione dei servizi da parte dell'azienda. Il documento descrive le varie fasi per provvedere al ripristino del sistema di telecomunicazione, al recupero dei dati e alla configurazione delle procedure per gestire l'emergenza e avviare il ritorno alle normali condizioni operative. Sono inoltre incluse le procedure per l'attivazione

del sito di DR (sede secondaria) nel caso in cui il sito primario non sia accessibile e utilizzabile.

L'azienda ha anche effettuato un'analisi delle minacce possibili e dei relativi rischi che possono derivare sia da una non corretta gestione dell'infrastruttura informatica, sia dall'integrità delle apparecchiature elettroniche e informatiche. La sicurezza e l'integrità dei dati, in termini di protezione da varie tipologie di cause, esterne e interne all'azienda, permettono di raggiungere livelli di sicurezza tali da garantire una drastica diminuzione delle probabilità di rischio.

L'integrità fisica dei sistemi informatici e di telecomunicazione, può essere compromessa o distrutta da:

- Calamità naturali (alluvioni, terremoti, fulmini, ecc.)

- Cause accidentali (incidenti, allagamenti, distruzione dell'edificio, distruzione di personal computer, server o altri dispositivi elettronici che contengono i dati trattati)

- Cause esterne (sommosse, rivolte, devastazioni, atti vandalici, eventi socio-politici, furti)

L'integrità fisica delle infrastrutture, descritta nei paragrafi successivi, è essenziale per il funzionamento dei sistemi e per garantire una normale attività lavorativa agli operatori dell'azienda. Questa integrità deve essere assicurata dalla continua fornitura di elettricità nello stabile. Per far fronte a eventuali interruzioni temporanee di energia elettrica e cali di tensione, sono previsti Dispositivi UPS (Gruppi di Continuità), in grado di intervenire in caso di guasti, garantendo un’autonomia operativa di 30 minuti.

L'integrità dei dati, fondamentale per lo svolgimento del servizio, deve sempre essere garantita e può essere compromessa da errori umani del personale, guasti dell'hardware, interruzioni della connessione internet, furto di dati o credenziali di accesso al sistema, e azioni di hacking.

Per limitare la perdita o l'alterazione dei dati, è necessario predisporre minimi livelli di sicurezza e garantire un backup dei dati trattati in modo corretto e costante.

2. DESCRIZIONE DELLA SOLUZIONE DI DISASTER RECOVERY

In questa sezione viene descritta la soluzione di disaster recovery adottata dall'azienda per garantire la continuità operativa del sistema informatico e telematico in caso di eventi dannosi che causino un'indisponibilità del servizio oltre la soglia di tolleranza.

La scelta di utilizzare un sito di DR su "Cloud" è stata motivata da condizioni operative che offrono un rapporto costi/benefici ottimale, considerando i seguenti elementi:

- Volume medio-basso di dati da mantenere sul sito Cloud.

- Variazione giornaliera dei dati che permette la trasmissione attraverso le linee internet disponibili all'azienda.

Per quanto riguarda il Disaster Recovery, la soluzione di "Cloud Computing" è stata adottata per le seguenti attività:

- **Posta elettronica Outlook**: l'azienda ha attivato delle licenze Microsoft per i propri dipendenti, includendo la posta elettronica Outlook. La posta è installata su tutti i PC dei dipendenti, costantemente aggiornata e archiviata online sul cloud Microsoft, accessibile tramite internet con le credenziali dei vari profili.

- **Google Drive**: i dati archiviati nello storage sono sincronizzati con Google Drive, su cui l'azienda dispone di uno spazio di archiviazione di 100 GB. Questo spazio è sufficiente per le attuali esigenze, ma può essere ampliato se necessario per garantire il backup in cloud di tutti i dati gestiti dall'azienda (sia per il servizio di customer support che per gli altri servizi). Google Drive consente il recupero illimitato dei file (possibilità di recuperare file precedenti senza limite temporale) e offre la possibilità di avere più utenze collegate all'azienda, con accessi diversificati ai vari contenuti archiviati, secondo i diritti di accesso definiti dall'azienda.

Per quanto riguarda i programmi utilizzati per erogare il servizio di customer support (es. software per il tracking delle segnalazioni, software per il recupero delle password degli utenti iscritti, ecc.) e le piattaforme telematiche interessate dal servizio, essi sono accessibili online. Queste applicazioni funzionano su internet e l'accesso è regolato tramite credenziali fornite dai proprietari dei programmi/piattaforme. Anche per i dati gestiti su questi programmi e piattaforme, l'attività di disaster recovery è garantita dalle aziende proprietarie e/o fornitrici dei servizi.

La criticità del piano di Disaster Recovery dell'azienda si basa quindi prevalentemente sulla disponibilità e qualità del collegamento internet per accedere agli archivi/software di tipo cloud e sulla qualità della rete telefonica.

3. POLITICA DI SICUREZZA E DI SALVAGUARDIA DEI DATI

In questa sezione vengono delineate le procedure di backup e archiviazione dei dati adottate dall'azienda per prevenire la perdita dei dati e garantire la loro salvaguardia attraverso la copia conservata in cloud.

Il backup rappresenta un punto cruciale nelle procedure di disaster recovery e per aumentare i livelli di sicurezza è essenziale che le copie di sicurezza dei dati siano conservate anche al di fuori della sede dell'azienda, ovvero nel cloud.

L'azienda si è dotata di un'infrastruttura hardware supportata da un ambiente software specifico e servizi cloud, organizzati come segue:

- Uno storage situato nella sede principale e un altro di ridondanza nell'ufficio adiacente, sincronizzati tra loro una volta al giorno. Il server primario è sempre istantaneamente sincronizzato con il cloud di Google Drive.

- Gli operatori del customer support gestiscono direttamente i dati sulle cartelle connesse allo storage e i dati vengono salvati direttamente su di esso.

- Ogni giorno viene eseguito automaticamente il backup dei dati contenuti nello storage anche su un altro hardware.

- In tempo reale, avviene la sincronizzazione di tutti i dati dello storage sul cloud. Il cloud utilizzato dall'azienda è Google Drive.

- Le email sono gestite e conservate nel cloud di Microsoft, oltre ad essere presenti in locale sui PC degli utenti e scaricate settimanalmente su un ulteriore hardware.

- Per quanto riguarda i dati gestiti tramite piattaforme telematiche utilizzate per il servizio di customer support e/o attraverso software gestionali forniti dai clienti per l'erogazione del servizio stesso, essi sono archiviati e gestiti dai fornitori/proprietari delle piattaforme stesse.

4. FASI DELLA SOLUZIONE DI DISASTER RECOVERY

- Valutazione della situazione di crisi/disastro/indisponibilità del sito primario.
- Dichiarazione del Disastro da parte del RCO.
- Notifica e attivazione delle strutture e del personale coinvolto nelle attività connesse alla dichiarazione di Disastro.
- Attivazione del piano DR.
- Attivazione del sito di DR e verifica del funzionamento del sistema informativo.
- Gestione del sistema informativo presso il sito di DR.
- Ripristino della sede primaria.

5. GESTIONE E AGGIORNAMENTO DEL PIANO DR

L'aggiornamento e la revisione del piano di DR sono di primaria importanza per assicurare la sua costante adattabilità alle attività e all'organizzazione dell'azienda. Questo processo è garantito da una verifica periodica dell'adeguatezza della soluzione di DR da parte del Responsabile della Continuità Operativa. Il Responsabile è anche responsabile di verificare l'aggiornamento regolare dei piani e degli allegati, la formazione del personale indicata nei documenti e l'esecuzione di testing ed esercitazioni.

I servizi di assistenza software, hardware e TLC hanno l'obbligo di segnalare preventivamente al Responsabile della Continuità Operativa qualsiasi cambiamento tecnologico che potrebbe rendere inapplicabile il piano di DR, variazioni significative nelle criticità dei processi gestiti e, in particolare, nel RTO. Questo permette di modificare strategie, piani e soluzioni tecnologiche contenute nel piano stesso per adeguarli alla nuova situazione.

6. FORMAZIONE SUL PIANO BC E DR

L'azienda fornisce formazione ai dipendenti coinvolti nel servizio soggetto al presente Piano, con una frequenza annuale e ogni volta che il Piano viene modificato.