DOCUMENTO PROGRAMMATICO SICUREZZA

DPS

www.ediliziaetecnologia.it

edilizia e tecnologia

Indice

1. PIANO DI CONTINUITÀ OPERATIVA

1.1 Obiettivi e ambito di applicazione

La nostra Organizzazione si è dotata di un Piano di Continuità Operativa (BCP) e Disaster Recovery (DR) al fine di disporre di procedure atte a gestire e superare condizioni di emergenza e di disastro che impediscono la normale erogazione dei suoi servizi.
In particolare, al verificarsi di un'emergenza e/o disastro, deve essere garantito:

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

Il presente Piano di Continuità Operativa documentato (BCP) racchiude tutte le informazioni e procedure necessarie per la gestione di eventi straordinari che compromettano l'ordinaria attività lavorativa della Società.
Il BCP prevede al suo interno una sezione appositamente dedicata del Piano di Disaster Recovery (DR) che definisce i possibili disastri e gli scenari di rischio, individua i processi critici e le figure di riferimento, interne ed esterne alla Società, in caso di gravi problemi oltre che le modalità di risoluzione degli stessi.
Tutti i dipendenti sono a conoscenza delle procedure da mettere in atto per affrontare la condizione di disastro e/o emergenza in modo che possano continuare la loro attività in caso di incidente.
Il presente documento è finalizzato a illustrare le modalità tecnico/organizzative a cui la Società deve attenersi per garantire l'operatività dei propri servizi, rispettando un predeterminato periodo di tempo, a seguito di disastro o grave evento dannoso.
Nella redazione del Piano di Continuità Operativa la Società ha cercato di analizzare e ridurre le cause di rischio e ha aumentato i livelli di sicurezza delle proprie strutture. Il Piano in oggetto racchiude quindi tutte le informazioni legate all'organizzazione logistica della Società, dalla dichiarazione dell'emergenza al rientro alla normalità fino alle metodologie atte a riconoscere una situazione di crisi e far così fronte alla stessa. Tale Piano include i processi di gestione della crisi e del disaster recovery cioè le procedure riferite alle modalità di ripristino delle attività per garantire la prosecuzione dell'erogazione dei servizi.
Il presente Piano permette di stabilire quali siano le procedure alternative da attuare in caso di disastro per garantire l'operatività della Società, attraverso i test periodici e l'efficacia delle procedure di ripristino.
Il Piano di Continuità Operativa valuta la criticità del servizio prevedendo le strategie di ripristino: sito alternativo, metodologie per il backup, apparecchiature per il backup, ruoli e responsabilità delle figure coinvolte. Particolare attenzione viene data all'interno del BCP alla definizione degli scenari di disastro in quanto il non tempestivo riconoscimento della gravità della situazione venutasi a creare può determinare un ritardo irrecuperabile nella dichiarazione di emergenza e quindi nella gestione della stessa.
Il personale addetto al servizio ha, di norma, il compito di rilevare le condizioni di emergenza e di comunicarle al Responsabile dei Servizi IT che si attiverà nei tempi e nelle modalità previste dal presente Piano.
La Società dispone delle seguenti sedi operative:

- **Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari (BA)**

1.2 Ruoli e responsabilità

Le responsabilità nel processo decisionale durante l'emergenza competono al Responsabile dei Servizi IT (RSIT) che dovrà valutare l'emergenza e prendere le necessarie decisioni per provvedere al rientro dall'emergenza stessa.
Il RSIT è l'organismo di vertice nella gestione delle crisi a cui spettano le principali decisioni e la supervisione delle attività delle eventuali risorse coinvolte. È l'organo di direzione strategica dell'intera struttura in

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

occasione dell'apertura della crisi e, inoltre, ha la responsabilità di garanzia e controllo nell'attuazione del Piano BC e DR.
Le decisioni del RSIT saranno documentate in apposita relazione nel momento in cui sarà conclusa l'emergenza La relazione dovrà recare tutte le informazioni relative all'attivazione del processo di continuità operativa e alla dichiarazione di rientro dall'emergenza.

Attualmente, il Responsabile dei Servizi IT è Devitofrancesco Vincenzo mail: ediliziaetecnologiasrl@gmail.com – cell. +39 348 3202846

Il RSIT si occupa di:

- Definizione, approvazione e aggiornamento del Piano di Continuità Operativa;
- Valutazione delle situazioni di emergenza e dichiarazione dello stato di crisi;
- Avvio delle attività di recupero e controllo del loro svolgimento;
- Rapporti con l'esterno e comunicazioni ai dipendenti;
- Avvio delle attività di rientro alle condizioni normali e controllo del loro svolgimento;
- Dichiarazione di rientro;
- Gestione di tutte le situazioni non contemplate ma necessarie per la corretta attuazione del BCP;
- Promozione e coordinamento delle attività di formazione e sensibilizzazione sul tema della continuità operativa.

In condizioni di incidente disastroso, il RSIT assume il controllo di tutte le operazioni e la responsabilità sulle decisioni per affrontare l'emergenza, ridurne l'impatto e soprattutto ripristinare le condizioni preesistenti.
Il RSIT deve essere supportato dalle altre figure presenti in azienda e dal personale stesso, ove necessario, per garantire il funzionamento del BCP in relazione alle seguenti attività:

- supporto negli eventuali spostamenti;
- per garantire il funzionamento e l'accesso a tutte le infrastrutture informatiche e di telecomunicazioni predisposte;
- aggiornamenti relativi alle notizie provenienti dai canali pubblici di comunicazione;
- esame di tutti gli aspetti di sicurezza, in particolare per quanto riguarda la verifica del grado di sicurezza offerto dalle configurazioni adottate per l'emergenza e la protezione dei dati, o tramite il riesame delle soluzioni adottate per il ripristino dei sistemi e per il rientro alla normalità.

Il RSIT ha il compito di provvedere agli aggiornamenti del Piano di Continuità Operativa e del Piano di Disaster Recovery.
In caso di dichiarazione di disastro/emergenza il RSIT provvede, inoltre, a redigere una relazione che illustri le fasi e l'evoluzione dell'emergenza che sarà archiviata nell'archivio informatico della Società e che sarà inviata ai soggetti (es. Stazioni Appaltanti ed Operatori Economici) che sono stati interessati dall'attivazione del Piano BC e DR.

1.3 Gli strumenti di telecomunicazione

Gli strumenti TLC utilizzati dalla nostra Società comprendono: pc, telefoni collegati alla rete fissa, telefoni collegati alla rete mobile, collegamento internet 20 mega con 512 K garantiti.
La sede 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 ne garantisce la funzionalità in caso di abbassamenti, innalzamenti o assenza di tensione, per circa 30 minuti.
Nello specifico, la nostra sede dispone complessivamente di 8 canali di Fonia (Linee telefoniche) ripartite in 4 diversi collegamenti BRI ISDN 2 canali ciascuno, il tutto gestito da un Sistema Centralizzato VOIP con alta affidabilità data da due Hardware fisici con le stesse capacità situati in sedi diverse capaci di sostituirsi a vicenda.
I dipendenti dispongono ciascuno di un computer fisso collegato alla rete aziendale per erogare il servizio.

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

Ogni computer è dotato di un accesso in locale alle caselle e-mail dedicate al servizio, con relativa archiviazione.
In caso di evento dannoso, la continuità operativa è garantita con le seguenti modalità:

- Linee telefoniche: i dipendenti dispongono di cellulari di servizio da utilizzare in caso di indisponibilità della rete fissa da parte dell'Operatore.
- Linea internet: in caso di indisponibilità di collegamento, gli operatori sono dotati di router portatile per collegarsi a Internet in UMTS e continuare a erogare il servizio.
- Computer: nella sede sono disponibili pc portatili, in dotazione agli addetti al servizio, programmati con i software e gli accessi necessari (es. piattaforme, posta, software) per garantire l'operatività del servizio tramite una pronta sostituzione dei pc fissi qualora manchi la corrente elettrica, garantendo un'autonomia di circa 2 ore per pc. A tale scopo, le batterie dei pc portatili sono verificate sistematicamente, a cadenza settimanale e, ove necessario, ricaricate.

1.4 Servizio di archiviazione e attività di recupero dati

Tutti i dati acquisiti durante lo svolgimento del servizio, unitamente agli altri dati prodotti/acquisiti dalla Società, sono archiviati in tempo reale su uno "Storage", dotato di backup automatico e in cloud. Il salvataggio dei dati viene altresì replicato quotidianamente, sempre in modalità automatica, in ulteriore Hardware (PC fissi, Hard-disk USB, storage secondario).
Lo storage contiene lo storico dei salvataggi di una settimana: questo garantisce che in caso di perdita accidentale dei dati salvati all'interno dello stesso, sia possibile recuperarli accedendo all'ultimo salvataggio effettuato.
Anche lo storage secondario è sincronizzato al cloud, che garantisce un back up automatico in tempo reale di tutti i dati contenuti al suo interno.
Specifichiamo che per i dati archiviati in cloud, il *disaster recovery* è garantito dai proprietari degli stessi, come specificato nella successiva Parte B.
Per quanto riguarda la posta elettronica (in entrata e in uscita), è archiviata in cloud ed è altresì replicata su un hardware con un back up settimanale.
Ogni pc utilizzato dalla Società è dotato di un firewall software. Per garantire un maggior grado di sicurezza dei dati, è stato installato anche un firewall hardware.

1.5 Tempi di recupero dei servizi (RTO)

L'RTO, acronimo inglese di Recovery Time Objective, rappresenta il tempo massimo accettabile per operare il ripristino dei servizi, senza determinare un disservizio altrimenti non recuperabile in termini di qualitativi.
Il RTO è fissato in 60 minuti, rilevato come il lasso di tempo necessario per ripristinare l'operatività del servizio attraverso la riattivazione delle TLC, come indicato al precedente par. 1.3.

1.6 Livelli di recupero necessario per ogni servizio (RPO)

L'RPO, acronimo inglese di Recovery Point Objective, rappresenta la massima perdita di dati tollerata: è quindi il valore che descrive la differenza tra il momento in cui il dato viene prodotto e la sua messa in sicurezza attraverso opportune procedure di backup e/o copia sul sito di DR.
I dati prodotti e gestiti dai dipendenti sono delle seguenti tipologie:

- Telefonate: l'entità delle telefonate, il numero, il contenuto di riferimento vengono registrate quotidianamente dagli addetti su un calendar condiviso in cloud Microsoft e archiviate automaticamente in tempo reale (oppure: la registrazione avviene settimanalmente in un file riepilogativo direttamente su storage).

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

• E-mail: sono archiviate in locale sui singoli pc degli addetti e in cloud in maniera istantanea al loro invio/ricezione. Settimanalmente, tutte le e-mail sono salvate in automatico in un Hardware di back-up.
• Altri documenti prodotti/gestiti durante lo svolgimento del servizio sono realizzati e/o archiviati operando direttamente sulle cartelle di file dello storage con back-up automatico sul cloud Google Drive.
Come descritto al precedente paragrafo 1.3, il back up su storage e sul cloud avviene in tempo reale e automaticamente. Questo permette di avere dati costantemente archiviati e aggiornati sia in locale che in cloud.

1.7 Cause di attuazione del piano – Scenari di crisi

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

1. Indisponibilità della sede per eventi atmosferici, allagamenti, incendi, etc.;
2. Indisponibilità della sede per:
   a. Indisponibilità o assenza prolungata dell'energia elettrica;
   b. Indisponibilità o assenza prolungata della rete per il trasferimento dei dati (internet);
   c. Indisponibilità o assenza prolungata della rete per la telefonia fissa.
3. Mancanza massiva di personale dovuta, a titolo esemplificativo, a epidemia influenzale o strade bloccate.
4. Perdita documentazione

Ogni dipendente che riscontri un problema e/o un disservizio che impedisca il normale svolgimento dell'attività lavorativa, sia esso logistico o informatico o legato al personale, deve informare il proprio Responsabile.
Il Responsabile valuterà la situazione sottoposta dal dipendente; nel caso in cui il problema non sia risolvibile con gli ordinari mezzi di intervento attiverà il RSIT.
In particolare, il RSIT è tenuto ad utilizzare la "Tabella di classificazione degli incidenti", di cui al successivo par. 1.8, per determinare il grado di severità dell'incidente ("Grave" o "Disastroso").
In base al livello di gravità delle condizioni riscontrate, si potranno/dovranno prendere le seguenti decisioni:

1. Indisponibilità della sede per eventi atmosferici, allagamenti, incendi, etc.
2. Indisponibilità della sede per:
   a. Indisponibilità o assenza prolungata dell'energia elettrica;
   b. Indisponibilità o assenza prolungata della rete per il trasferimento dei dati (internet);
   c. Indisponibilità o assenza prolungata della rete per la telefonia fissa.

In questi casi, se l'indisponibilità si protrae oltre 15 minuti, il RSIT attiva le procedure di cui al precedente par. 1.3.

3. Indisponibilità di personale essenziale: mancanza massiva di personale.

Questa è la casistica di più complessa gestione, in quanto il personale è specializzato per l'erogazione del rispettivo servizio cui è addetto. In caso di eventi eccezionali (es. pandemie influenzali, blocchi delle strade di accesso alla sede prolungati) che comportano l'assenza massiva di personale, la contromisura che il RSIT può prendere è: *Ricorrere al restante personale dipendente della Società* per supplire temporaneamente alla carenza degli addetti assenti.
4. Perdita di documentazione: archiviando tutti i dati e i documenti in cloud, questo scenario non è ritenuto plausibile.

1.8 Tabella di classificazione degli incidenti

Il RSIT è tenuto a utilizzare la seguente tabella per determinare il grado di severità dell'incidente:

Livello	Classe incidente	Descrizione	Responsabilità

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

1	ORDINARIO	L'incidente non provoca disservizi significativi e l'impatto sull'operatività della Società non è rilevante. L'evento è risolvibile con mezzi di intervento ordinari	Responsabile del servizio o suo delegato
2	SIGNIFICATIVO	Degrado o interruzione di una percentuale minoritaria (< 25%) del servizio per cui lo stesso continua ad essere erogato anche se in modalità rallentata	Responsabile del servizio o suo Delegato
3	GRAVE	Degrado o interruzione di una percentuale da media a elevata (26% < x < 55%) del servizio per cui lo stesso continua ad essere erogato ma causando gravi disservizi	RSIT
4	DISASTROSO	Incidente che causa l'interruzione di una percentuale da elevata a completa del servizio (56% < x < 100%)	RSIT

1.9. Modalità di attivazione, gestione e manutenzione del BCP

La dichiarazione dello stato di crisi e l'attivazione del presente Piano di BC è compito del RSIT che assicura anche la gestione delle fasi successive di recovery descritte nei capitoli a seguire.
Le modalità per cui si deve attivare il piano di continuità operativa sono regolamentate in questa sezione. Vengono di seguito elencati i casi limite in cui deve essere attivato il piano in modo che i dipendenti della Società sappiano valutare immediatamente il livello del disservizio.
Risulta infatti decisiva la corretta valutazione della gravità dell'evento in modo da attuare subito il piano idoneo ad arginare l'emergenza.
A tal proposito tutti i dipendenti della Società e i fornitori con cui la Società ha stipulato contratti di assistenza hardware e software, hanno conoscenza del Piano BC e il Piano di DR.
Il piano include:

1. Modalità di mobilitazione delle persone interessate;
2. Punti di ritrovo;
3. Circostanze in cui l'organizzazione ritiene che l'attivazione del BCP non sia necessaria;
4. Modalità di gestione, manutenzione, verifica e test del BCP;
5. Piano di Disaster Recovery;
6. Modalità di rientro dall'emergenza.

I punti sopra elencati sono sviluppati nei prossimi paragrafi.

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

1.9.1 Modalità di mobilitazione delle persone interessate

Il RSIT e le altre figure interessate nell'attivazione del Piano di Continuità Operativa e di Disaster Recovery, interni ed esterni alla Società, devono essere tempestivamente contattati attraverso i canali di comunicazione più rapidi.

1.9.2 Punti di ritrovo

Il punto di ritrovo principale è la sede della Società sita in Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari (BA).
Nel caso in cui non sia possibile operare presso il sito primario, il RSIT dichiarerà e organizzerà lo spostamento del personale e delle infrastrutture trasportabili presso una sede secondaria agibile e adeguatamente attrezzata.

1.9.3 Circostanze in cui l'organizzazione ritiene che l'attivazione del BCP non sia necessaria

Nei casi in cui l'interruzione parziale e temporanea del servizio non comporti perdite di dati o disservizi rilevanti (vedi Tabella di classificazione degli incidenti) non sarà necessario attivare il Piano di Continuità Operativa.

1.9.4 Modalità di gestione, manutenzione, verifica e test del Piano BC e DR

Il Piano BC e DR sarà aggiornato periodicamente dal RSIT secondo necessità (a titolo esemplificativo e non esaustivo: modifica delle condizioni di erogazione del servizio, etc.).
In ogni caso, il Piano di Continuità Operativa dovrà essere aggiornato almeno una volta ogni due anni.
Qualsiasi modifica apportata al Piano di Continuità Operativa e/o al Piano di Disaster Recovery costituisce revisione del Piano stesso e pertanto deve essere archiviata. Ciascuna versione del Piano dovrà avere un numero identificativo della data e della versione del piano.
Le copia del Piano di Continuità Operativa e del Piano di Disaster Recovery della Società, costantemente aggiornati, saranno depositate presso gli uffici della Società, oltre che salvate in maniera digitale sullo storage e notificate alle figure coinvolte nei piani stessi ad opera del RSIT.
Il Servizio di assistenza software e quello di assistenza hardware e TLC sono tenuti a segnalare preventivamente al RSIT ogni cambiamento tecnologico che possa rendere inapplicabile il presente documento, in modo da consentire di modificare i piani e le soluzioni tecnologiche ivi contenute.

1.9.5 Piano di Disaster Recovery (PDR)

Il PDR è contenuto all'interno del presente Piano di Continuità operativa e ne costituisce la Parte B.

1.9.6 Modalità di rientro dall'emergenza

Il ritorno allo svolgimento della normale attività lavorativa è la condizione in cui non risulta necessario prolungare l'adozione del Piano e di conseguenza la fine dell'emergenza. Il rientro dall'emergenza è deciso dal RSIT che valuta il disastro, dichiara l'emergenza, prende le decisioni durante tutto l'arco temporale della stessa e al termine di essa decide sul rientro, dopo aver valutato le condizioni di ripristino del servizio.
La dichiarazione di rientro dall'emergenza viene effettuata nel momento in cui l'erogazione del servizio raggiunga nuovamente la piena operatività.

2. PIANO DI DISASTER RECOVERY

Il Piano di Disaster Recovery, che fa parte integrante del BCP, è l'insieme delle azioni e dei sistemi con i quali la Società provvede al ripristino delle funzionalità tecnologiche e organizzative della propria struttura. Esso

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

contiene la descrizione delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione del servizio a fronte di gravi emergenze che ne intacchino la regolare attività.

2.1. 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 della Società.
Nel piano di DR vengono altresì dettagliate le procedure operative necessarie per effettuare una corretta valutazione della situazione di emergenza/disastro che non consenta la normale erogazione dei servizi da parte dell'Organizzazione. Nel presente documento vengono inoltre descritte le varie fasi per provvedere al ripristino del sistema di telecomunicazione, ovvero del recupero dei dati e la configurazione delle procedure per arginare l'emergenza e avviare il successivo rientro alle normali condizioni operative.
La Società ha anche provveduto all'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 degli stessi da varie tipologie di cause, esterne e interne alla Società, permette di raggiungere livelli di sicurezza che garantiscono una drastica diminuzione delle probabilità di rischio.
L'integrità fisica dei sistemi informatici e di telecomunicazione, infra dettagliata, può infatti essere intaccata o distrutta da:

- calamità naturali (alluvioni, terremoti, fulmini, etc.)
- cause accidentali (incidenti, allagamenti, distruzione dell'edificio, distruzione di personal computer, server o altri elaboratori elettronici in cui siano custoditi i dati trattati)
- cause esterne (sommosse, rivolte, devastazioni, atti vandalici, eventi socio-politici, furti)

L'integrità fisica delle infrastrutture, infra dettagliata, necessaria per il funzionamento dei sistemi e per poter consentire una normale attività lavorativa agli operatori della Società, deve essere assicurata dalla continua presenza dell'elettricità nello stabile. Per sopperire a mancanze temporanee di energia elettrica e cali di tensione, è prevista la disponibilità di Dispositivi UPS (Gruppi di Continuità), in grado di subentrare in caso di guasti di varia natura, che garantiscono un'autonomia operativa di 30 minuti, come specificato al precedente par. 1.3.
L'integrità fisica delle infrastrutture è altresì garantita dal fatto che la seda della società, sotto il profilo prevenzionistico, è conforme alle vigenti disposizioni in materia di igiene e sicurezza sul lavoro (D.Lgs. 81/2008) e di prevenzione incendi (DPR 157/2011 – D.M. 10/03/98).

L'integrità dei dati, indispensabile per lo svolgimento del servizio, deve sempre essere garantita e potrebbe essere compromessa da semplici errori umani del personale, da guasti dell'hardware, dal non funzionamento della connessione internet, da furto di dati o di credenziali di accesso al sistema, da azioni di *hacking*.
Per limitare la perdita dei dati o l'alterazione degli stessi è necessario predisporre minimi livelli di sicurezza e garantire un corretto e costante backup dei dati trattati, come meglio dettagliato nel paragrafo rubricato "Politiche di sicurezza e salvaguardia dei dati".

2.2 Descrizione della soluzione di disaster recovery

In questa sezione viene descritta la soluzione di disaster recovery adottata dalla Società per assicurare la continuità di funzionamento del sistema informatico e telematico a fronte di eventi dannosi che comportino un'indisponibilità del servizio oltre la soglia di tolleranza indicata al precedente par. 1.8.
La scelta di dotarsi di un sito di DR su "Cloud", è stata dettata da condizioni operative che permettono di sfruttare una soluzione con rapporto costi/benefici ottimali, tenendo conto dei seguenti elementi:

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

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

• Variazione giornaliera dei dati che permette la trasmissione attraverso le linee internet a disposizione della Società

In merito al Disaster Recovery, la soluzione "Cloud Computing" è stata adottata per le seguenti attività:

- **Posta elettronica Outlook**: la nostra Società ha attivato delle licenze Microsoft per i propri dipendenti, che comprendono anche la posta elettronica Outlook. La posta è installata su tutti i pc dei dipendenti della Società. La posta è costantemente aggiornata e archiviata on line sul cloud Microsoft e consultabile da internet, accedendo con le credenziali dei vari profili.
- **Google Drive**: i dati archiviati nello storage sono costantemente sincronizzati con Google Drive, su cui disponiamo di uno spazio di archiviazione di 100 GB. Lo spazio è ampiamente sufficiente per le nostre esigenze ma, nel caso in cui risulti necessario ampliarlo, sarà acquistato ulteriore spazio necessario per garantire il back-up in cloud di tutti i dati gestiti dalla Società. Google Drive consente il recupero dei file illimitato (cioè la possibilità recuperare file precedenti senza limite temporale) e di avere più utenze collegate alla Società, oltre che accessi diversificati ai vari contenuti archiviati, a seconda dei diritti di accesso definiti dalla Società.

Per i suddetti software e i relativi piani DR, si rimanda alle specifiche aziende fornitrici dei servizi.

La criticità legata al piano di Disaster Recovery della Società è quindi basato prevalentemente sulla disponibilità e qualità del collegamento internet per accedere agli archivi/software di tipo cloud e di quello telefonico.
Per questa ragione, la Società:

• per garantire e migliorare il proprio sistema informatico, ha provveduto a stipulare un contratto di manutenzione e assistenza tecnica software con la ditta ABC …….S.r.l. che prevede un supporto sia programmato che on demand che garantisce un intervento in caso di evento bloccante entro 2 ore lavorative dalla richiesta, tramite e-mail, telefono e/o con la presenza in loco dei propri tecnici qualora la problematica non sia risolvibile da remoto.

• ha attivato un contratto di assistenza tecnica per la parte hardware degli apparati di telecomunicazione, con la ditta DFG …….S.r.l. che garantisce il ripristino dell'efficienza dei sistemi con tempistiche di intervento di due ore lavorative dalla richiesta, in caso di guasto di tipo bloccante, sia con interventi da remoto che on-site dei propri tecnici qualora necessario.

L'attivazione del piano di DR consiste quindi nel ripristinare l'accesso a internet e alla linea telefonica, condizioni necessarie per l'erogazione del servizio che sarà comunque garantito anche in caso di non fruibilità della linea fissa, nelle modalità indicate al precedente par. 1.3.

2.3. Perimetro di riferimento del piano

2.3.1 Descrizione del sistema informativo primario

La Società ha una sede sita in Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari (BA).
La Società possiede un proprio sistema informativo, ubicato all'interno della predetta sede, costituito da: storage, router, computer, centralino, canali fonia e dati, telefoni VOIP.
Tutti i pc dei dipendenti della Società possiedono un sistema antivirus e firewall software.
La società si è dotata di un firewall hardware.

2.3.2 Fattori critici e di rischio: elenco dei possibili rischi

In questa sezione vengono dettagliati i rischi possibili e probabili a cui possono essere sottoposte le infrastrutture, fisiche e tecnologiche della Società, e i dati trattati.

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

Per i dati trattati devono essere garantite le seguenti qualità fondamentali:

a) la **disponibilità**: assicura che l'accesso ai dati sia disponibile quando necessario. Per garantire questo, l'accesso alle informazioni o alle risorse informatiche è negato a chi non possiede l'autorizzazione;

b) l'**integrità**: garantisce l'accuratezza e completezza dei dati e delle informazioni custodite all'interno degli hardware ovvero nello storage. Per garantire questa "qualità" si rende necessario codificare ed adottare delle corrette procedure per il backup dei dati e nel contempo evitare che le informazioni correttamente salvate possano formare oggetto di modifica o di accesso senza autorizzazione;

c) la **riservatezza**: garantisce che i dati e le informazioni siano conosciute e accessibili solo ed esclusivamente al personale autorizzato. Il rispetto della citata "qualità" si ottiene negando l'accesso alle informazioni a tutti i soggetti, interni ovvero esterni alla Società, che non siano legittimati al trattamento e alla conoscenza degli stessi dati.

Per garantire il rispetto di queste qualità è necessario conoscere ed analizzare le minacce che potrebbero incidere sulle stesse.

Gli eventi in grado di determinare dei danni e, conseguentemente, in grado di rappresentare un rischio per la sicurezza dei dati trattati dall'Organizzazione, possono essere ricondotti a 3 macro-categorie:

A. EVENTI RICONDUCIBILI AL COMPORTAMENTO UMANO
B. EVENTI RICONDUCIBILI AGLI STRUMENTI INFORMATICI
C. EVENTI RICONDUCIBILI AL CONTESTO FISICO-AMBIENTALE-INFRASTRUTTURALE

A. EVENTI RICONDUCIBILI AL COMPORTAMENTO UMANO

A.01 Accesso non autorizzato ai dati personali trattati mediante il cosiddetto "impersonamento informatico".

Nelle ipotesi di accesso non autorizzato ai dati personali trattati dalla Società mediante "impersonamento Informatico", un soggetto non autorizzato (interno o esterno alla Società stessa), può accedere ai dati con le credenziali di autenticazione attribuite all'incaricato legittimato all'accesso, sostituendosi in tutto e per tutto al soggetto titolare delle stesse.

La concreta possibilità che si verifichi un'ipotesi di accesso non autorizzato a dati trattati su supporto informatico si può avvenire nelle seguenti situazioni:

I. distrazione o negligenza di un operatore il quale, per esempio, lascia incustodita la propria postazione di lavoro collegata ovvero non custodisce diligentemente le proprie credenziali di autenticazione

II. scambio delle password tra gli incaricati

III. carenza nel sistema e nelle procedure di attribuzione e gestione dei profili di autenticazione e di autorizzazione degli utenti.

L'accesso non autorizzato ai dati trattati dalla Società espone a ulteriori rischi di modifica non autorizzata, di danneggiamento, di mancanza di congruità, di perdita e di esportazione illegittima dei dati stessi.

Per ridurre i suddetti rischi, la Società:

- **in riferimento al punto I) e II)**, ha sensibilizzato i propri operatori, con appositi ordini di servizio, oltre che con la diffusione del proprio codice disciplinare interno, a custodire e non diffondere le proprie credenziali di accesso sia ai computer che agli applicativi utilizzati, oltre che a non lasciare incustodita la propria postazione di lavoro se prima non ha provveduto alla disconnessione della propria utenza.
- **in riferimento al punto III)**, sono stati creati gruppi di utenza abilitati alle singole aree informatiche/di archiviazione di competenza. Per quanto riguarda l'accesso ai software oggetto del servizio, le password sono state rilasciate dai proprietari e/o gestori delle stesse, devono contenere caratteri alfanumerici e speciali e devono essere aggiornate periodicamente.

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

A.02 Insufficiente conoscenza del sistema informatico o dell'applicazione

In alcuni casi, l'operatore può involontariamente compiere azioni che causano un danno semplicemente perché non è perfettamente a conoscenza delle conseguenze del suo operato a causa di una non perfetta conoscenza del sistema, dello strumento informatico ovvero dell'applicazione.
Il danno che può essere provocato varia a seconda del comportamento posto in essere e può determinare:

i. Un blocco momentaneo della stazione di lavoro
ii. Un blocco che può coinvolgere anche altri utenti della Rete
iii. L'inserimento, la modifica o la cancellazione (e dunque la perdita) non voluta di informazioni e dati
iv. L'invio di dati a soggetti non autorizzati
v. La visione di dati a soggetti non autorizzati

Questa casistica è alquanto improbabile dal momento che gli operatori sono specializzati per lo svolgimento della propria attività. I nuovi operatori sono adeguatamente formati e affiancati da operatori esperti. Sono inoltre coordinati da un Responsabile che interviene in caso di necessità

A.03 Insufficiente conoscenza dei rischi e delle misure di sicurezza

Una non puntuale conoscenza dei gravi rischi che possono determinarsi quale conseguenza di una condotta non improntata al rispetto delle norme tecniche dettate dal Regolamento UE 2016/679 e dal D.Lgs. 196/03 s.m.i. può comportare i seguenti rischi:

i. La diffusione nell'ambito dell'Organizzazione, tra colleghi, delle credenziali di accesso
ii. La negligente custodia delle credenziali di autenticazione da parte del singolo operatore
iii. La circostanza che venga lasciata la propria stazione di lavoro accesa e collegata quando ci si allontana per qualsiasi ragione
iv. La circostanza che vengano lasciate, liberamente fruibili, stampe e tabulati contenenti dati riservati

Il danno che può essere determinato nelle ipotesi considerate è quello di accesso non autorizzato ai dati trattati, di modifica e di esportazione illegittima degli stessi e, nei casi più gravi, di distruzione.
In merito a tale comportamento la Società ha sensibilizzato i propri operatori, con appositi ordini di servizio oltre che con la diffusione del proprio codice disciplinare interno, a custodire e non diffondere le proprie credenziali di accesso sia ai computer che agli applicativi utilizzati, oltre che a non lasciare incustodita la propria postazione di lavoro se prima non ha provveduto a scollegare la propria utenza.

A.04 Distrazione e Negligenza

La distrazione e la negligenza possono essere di tipo "fisico" o "logico".
La distrazione/negligenza di tipo fisico, in genere, comporta direttamente danni alla strumentazione e alle attrezzature (es. rottura, danneggiamento, etc.) e, in alcuni casi, causa indirettamente danni ai dati.
La distrazione/negligenza di tipo logico invece, determina in genere esclusivamente danni ai dati trattati (a titolo esemplificativo e non esaustivo: durante la sessione di lavoro l'operatore viene distratto e dimentica di salvare il documento su cui stava lavorando o preme inavvertitamente dei tasti che provocano l'esecuzione di un comando non voluto).
Il danno che tale evento può determinare è quello di alterazione, corruzione, cancellazione e, nei casi più gravi, perdita dei dati.
In merito a tale evenienza, la Società cerca di garantire un ambiente lavorativo ordinato (per ridurre il rischio fisico) e tranquillo, evitando il coinvolgimento degli operatori di customer support in attività diverse da quelle che stanno svolgendo (per limitare il rischio logico).

A.05 Atto doloso

È senza dubbio il più grave e pericoloso degli eventi dannosi legati al fattore umano in quanto presuppone una precisa volontà indirizzata alla manomissione ovvero alla distruzione delle strumentazioni o dei dati trattati.

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

Potrebbe verificarsi che, con comportamento consapevole, derivante potenzialmente da vari fattori (es. risentimento verso la Società o perseguimento di fini personali), gli operatori compiano operazioni illecite durante l'erogazione del servizio.
Per ridurre questa tipologia di rischio, la Società si impegna a mantenere con tutti i propri dipendenti un rapporto di leale collaborazione, garantendo il rispetto dei diritti dei lavoratori e il mantenimento di un ambiente di lavoro sereno.

B. EVENTI RICONDUCIBILI AGLI STRUMENTI INFORMATICI

B.01 Azione di virus informatici ovvero di programmi suscettibili di recare danno

Esistono dei virus informatici programmati per cancellare o danneggiare i dati, o per causare la paralisi dei servizi erogati mediante gli strumenti informatici.
L'azione di questi agenti dannosi è generalmente innescata dal download di programmi di varia natura che vengono diffusi per posta elettronica sotto forma di allegati, oppure provengono da siti che, ingannando l'utente, lo inducono a salvare questi file sulla propria postazione di lavoro.
In merito a tale minaccia la Società ha impostato un sistema di antivirus e di firewall software per ogni pc. È stato anche attivato un firewall hardware.

B.02 Spamming o tecniche di sabotaggio

In riferimento ad azioni di sabotaggio compiute da terzi tramite programmi che sfruttando difetti del software utilizzato per la gestione della posta elettronica o di altri servizi informatici e saturano il servizio di richieste fino alla paralisi parziale o totale dello stesso. Questa azione determina l'indisponibilità temporanea dei dati gestiti dal servizio che forma oggetto di attacco.
In merito a tale minaccia la Società si avvale del Filtro Antispam del Client di posta elettronica e della protezione del Firewall hardware centrale.

B.03 Obsolescenza degli strumenti Hardware

L'obsolescenza delle attrezzature, che nel campo informatico è particolarmente rapida, oltre a rappresentare un fattore di rischio "attivo", può impedire l'attivazione e l'implementazione di misure di sicurezza fisiche o logiche che si rendano opportune per eliminare o ridurre alcuni rischi.
L'esempio che può essere fatto è quello che si riferisce all'impossibilità tecnica di installare su un vecchio pc un sistema di cifratura dei dati che richiede processori di una certa potenza e sufficiente memoria.
In merito al suddetto rischio, la Società, anche grazie agli incaricati dell'assistenza informatica e a quelli sugli apparecchi di telecomunicazione, provvede a monitorare il grado di obsolescenza delle proprie apparecchiature informatiche e a sostituirle con versioni più recenti in caso di necessità.

B.04 Malfunzionamento/indisponibilità degli strumenti Hardware

Come tutte le macchine, anche le strumentazioni informatiche sono soggette ad avarie che possono renderle inutilizzabili per periodi più o meno lunghi.
A seconda del tipo di guasto si può avere solo il blocco dell'attività della postazione di lavoro oppure anche il danneggiamento o la perdita dei dati (si pensi al caso di avaria che interessi l'hard disk).
Per far fronte a questa evenienza, la Società ha stipulato i contratti di assistenza con interventi "on demand" come specificato al precedente par. 2.2

B.05 Malfunzionamento Software e obsolescenza derivante da mancato aggiornamento

In questo punto si fa riferimento alla possibilità, insita in ogni software, di rivelare difetti di funzionamento inizialmente non presenti o non evidenti. Tale possibilità esiste sempre in quanto ogni programma dipende

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

da altri prodotti software (primo fra tutti il sistema operativo) e hardware (le apparecchiature di rete) che devono essere sostituiti o aggiornati nel tempo. Il risultato di tale evento può essere l'indisponibilità temporanea o addirittura permanente di dati nel caso più grave, in cui cioè non sia più possibile ristabilire la situazione originaria.
Anche per tale evento sono stati stipulati opportuni contratti di Aggiornamento Software con le aziende produttrici o intermediarie.

B.06 Accessi esterni non autorizzati

Questo è il caso in cui vi siano intrusioni via rete, avvenute senza furto di credenziali di autenticazione ma semplicemente mediante lo sfruttamento di difetti del software, per effettuare accessi non autorizzati ai dati. Ogni pc della Società è dotato di un firewall software. È stato anche installato un firewall hardware centralizzato di alta affidabilità che oltre ad impedire accessi dall'esterno ne traccia anche i tentativi.

C. EVENTI RICONDUCIBILI AL CONTESTO FISICO-AMBIENTALE-INFRASTRUTTURALE

C.01 Ingressi non autorizzati ad aree/locali ad accesso ristretto

In questo caso viene in rilievo la concreta possibilità che soggetti non legittimati possano materialmente introdursi all'interno dei locali e degli uffici in cui sono posizionati gli apparati e gli elaboratori informatici ospitanti i dati gestiti per l'erogazione del servizio. In casi di questo tipo, il danno che può derivare non è solo quello, di per sé già molto grave, di accesso di soggetto non autorizzato alle banche dati trattate dagli operatori, ma si possono verificare anche ipotesi di modifica, di distruzione e conseguente perdita, di esportazione illegittima delle banche dati oggetto dell'evento dannoso considerato.
In relazione a tale possibilità la Società ha provveduto alla protezione dei locali con apposite serrature le cui chiavi di accesso sono consegnate solo al personale dipendente. È altresì presente un sistema di allarme con sensori di movimento presenti in ogni stanza e agli accessi con batterie tampone della durata di 24 ore.

C.02 Sottrazione/Furto di strumenti contenenti dati personali

Ci si riferisce all'ipotesi di furto di una postazione di lavoro (workstation) ovvero di uno *storage* con conseguente perdita di tutti i dati ospitati nello strumento informatico oggetto di sottrazione.
Nell'ipotesi considerata, il danno provocato deriva da un soggetto non legittimato che accede alle banche dati ospitate all'interno dello strumento informatico con la conseguenza che la Società perda la disponibilità delle stesse.
In relazione a tale possibilità la Società ha provveduto alla protezione dei locali con apposite serrature le cui chiavi di accesso sono consegnate solo al personale dipendente. È altresì presente un sistema di allarme con sensori di movimento presenti in ogni stanza e agli accessi con batterie tampone della durata di 24 ore.
Si sottolinea inoltre che tutti i dati gestiti sono costantemente archiviati su storage che effettua una sincronizzazione automatica su cloud, quindi il furto del supporto hardware non comporta la perdita dei dati che possono sempre essere recuperati sull'archivio on-line.

C.03 Guasto a sistemi complementari (Impianto elettrico)

Ci si riferisce a tutti quegli eventi che riguardano sistemi e impianti esterni ma complementari agli strumenti informatici e che vanno ad impattare sugli stessi inficiandone la funzionalità. Il tipico esempio di guasto a sistema complementare è quello che riguarda l'impianto elettrico.
Il rischio correlato a tale tipologia di evento è quello di danneggiamento dei dati e di indisponibilità temporanea, ovvero nei casi più gravi, permanente degli stessi.
In relazione a tali guasti la Società è dotata di un sistema di UPS (Gruppi di Continuità) per poter continuare transitoriamente il lavoro durante l'eventuale black-out e attivare il piano di CO, come specificato al precedente par. 1.3.

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

C.04 Eventi distruttivi, naturali o artificiali accidentali o dovuti ad incuria

Include tutti gli eventi di effetto distruttivo sui supporti fisici contenenti i dati o sulle apparecchiature informatiche, indipendentemente dalla loro natura, qualora non siano già inclusi nelle casistiche precedenti. Il rischio che si può determinare sui dati è quello di danneggiamento, indisponibilità temporanea o perdita parziale o totale degli stessi.
Gli eventi in questione comprendono:

- Incendio parziale o diffuso
- Scariche atmosferiche
- Allagamenti
- Condizioni ambientali estreme

Fermo restando il fatto che la sede della Società è in regola con le normative antincendio e con quelle sulla sicurezza nei luoghi di lavoro, qualora si verifichino eventi che danneggino i supporti fisici di archiviazione questo non comporta la perdita dei dati in essi contenuti in quanto sono sincronizzati automaticamente con uno storage di tipo cloud.

C.05 Errori umani nella gestione della sicurezza fisica

Ci si riferisce a ogni evento determinato da un errore umano nella gestione della sicurezza negli ambienti fisici ospitanti gli apparati e gli strumenti informatici. In questa categoria sono ricomprese, a mero titolo esemplificativo, sia le ipotesi di non cura delle basilari norme di comportamento atte a garantire il non accesso di personale non autorizzato. Il rischio correlato a tale tipologia di evento va dall'accesso non autorizzato ai dati fino alla perdita e alla distruzione degli stessi.
Per ridurre questa tipologia di rischio, la Società sensibilizza periodicamente i propri dipendenti nell'osservanza delle regole di normale diligenza da utilizzare per garantire il corretto accesso ai locali.

2.3.3 Sicurezza Informatica

L'accesso al sistema informatico della Società e alle caselle di posta elettronica viene garantito attraverso la fornitura di apposite credenziali costituite da un codice identificativo (User ID) e da una password personali, attribuite in via esclusiva a ciascun dipendente; lo storage conserva tutte le informazioni sulle utenze e sui permessi di accesso alle risorse disponibili.
Le password devono essere aggiornate almeno ogni sei mesi, autonomamente da ciascun utente.
La forma di protezione adottata per contrastare gli eventuali sbalzi di tensione elettrica, come già menzionato al precedente par. 1.4, è rappresentata da gruppi di continuità collegati, in locale, ai computer della Società, allo storage e agli apparati di rete.
Come già anticipato nella sezione corrispondente, per la protezione da software dannosi, virus e malware, intrusioni dall'esterno, oltre all'installazione di antivirus e firewall software in tutti i Client di Rete (protezione locale), è stato installato un Firewall hardware centrale.

2.3.4 Descrizione dei casi di disastro/indisponibilità.

Casi in cui sarà attivata la soluzione di DR, rischi considerati:

- Mancanza di erogazione del servizio dovuta all'impossibilità di accedere ai dati e alle banche dati;
- Distruzione delle infrastrutture IT;
- Impossibilità di accedere ai locali destinati nei quali sono stati collocati: storage, apparati di rete e di backup;
- Indisponibilità dei servizi pubblici (esempio: rete elettrica, rete fonia, internet etc.).

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

2.4 Politica di sicurezza e di salvaguardia dei dati

In questa sezione vengono descritte le procedure di backup e archiviazione dei dati poste in essere dalla Società per evitare una qualsiasi perdita dei dati e di salvaguardia degli stessi attraverso la copia custodita in cloud.
Il backup è un punto fondamentale nelle procedure di disaster recovery e per garantire maggiori livelli di sicurezza è necessario che le copie di sicurezza dei dati siano collocate anche all'esterno della sede della Società, ovvero in cloud.
La Società, come meglio descritto in precedenza, per provvedere alla conservazione dei propri dati si è dotato di un'infrastruttura hardware, coadiuvata da specifico ambiente software e da servizi cloud, come di seguito organizzata:

- uno storage collocato nella sede e uno di ridondanza collocato ……. che sono tra loro sincronizzati una volta al giorno. Il server primario è sempre sincronizzato istantaneamente con il cloud Google Drive;
- gli utenti gestiscono i dati direttamente sulle cartelle collegate in linea con lo storage e i dati sono salvati direttamente sullo stesso;
- quotidianamente viene attuato in automatico il back-up dei dati contenuti nello storage anche su altro hardware;
- in tempo reale, avviene la sincronizzazione di tutti i dati contenuti nello storage sul cloud. Come indicato in narrativa, il cloud utilizzato dalla Società è Google Drive.
- per quanto riguarda le e-mail, sono gestite e conservate nel cloud Microsoft, oltre che in locale sui pc degli utenti e scaricate settimanalmente su un ulteriore hardware.
- in relazione ai dati gestiti attraverso software gestionali che ci sono stati messi a disposizione dai nostri fornitori per l'erogazione del servizio, questi sono archiviati e gestiti dai fornitori/proprietari degli stessi.

2.5 Fasi della soluzione di disaster recovery

Di seguito sono riepilogate le fasi della soluzione di disaster recovery individuata dalla Società:

I. Valutazione della situazione di crisi/disastro/indisponibilità sito primario
II. Dichiarazione del Disastro a opera del RSIT
III. Notifica e attivazione delle strutture e del personale coinvolto nelle attività connesse alla dichiarazione di Disastro
IV. Attivazione del piano DR
V. Attivazione del sito di DR e verifica del funzionamento del sistema informativo
VI. Gestione del sistema informativo presso il sito di DR
VII. Ripristino della sede con la formale "Dichiarazione di fine emergenza" da parte del RSIT

2.6 Gestione e aggiornamento del Piano DR

Di primaria importanza è l'aggiornamento/revisione del piano di DR affinché sia sempre adeguato all'attività e all'organizzazione della Società. Ciò è garantito da una verifica periodica dell'adeguatezza della soluzione di DR ad opera del RSIT, che è altresì tenuto a verificare l'aggiornamento periodico dei piani e degli allegati, la formazione del personale citato nei documenti, l'effettuazione di testing ed esercitazioni.
I servizi di assistenza software e di assistenza hardware e TLC sono tenuti a segnalare preventivamente al RSIT ogni cambiamento tecnologico che possa rendere inapplicabile il presente documento, variazioni rilevanti nelle criticità dei processi gestiti, in modo da modificare strategia, piani e soluzioni tecnologiche contenute nel piano stesso per adeguarli alla nuova situazione.

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

2.7 Procedure di test

La Società provvede all'esecuzione di test periodici e operativi in modo che sia garantito l'aggiornamento e il controllo dei piani. I test sono programmati almeno ogni sei mesi e comunque ogniqualvolta il Piano sia modificato.
Le modifiche del piano di Disaster Recovery saranno effettuate ogni qualvolta venga acquistata una nuova apparecchiatura per l'adeguamento del sistema informatico che vada a impattare sull'attuazione della soluzione tecnologica. Oltre all'adeguamento tecnologico del sistema informatico, si dovrà provvedere all'aggiornamento del Piano di DR anche nel caso in cui sia modificata la metodologia utilizzata per il disaster recovery.
I test periodici dovranno essere relazionati e inseriti nel Piano.
Possono comunque verificarsi condizioni che richiedono specifiche procedure di manutenzione straordinaria per cui si dovrà provvedere ad un adeguamento del Piano, a titolo esemplificativo e non esaustivo:

- modifiche dei Responsabili delle Aree/Servizi;
- modifiche legate ai gestionali utilizzati dalla Società e/o dal fornitore;
- modifica del fornitore dei servizi di assistenza hardware;
- modifica del fornitore dei servizi di assistenza software;

Alla conclusione delle procedure di test deve essere redatta una relazione, a cura del RSIT e conservata agli atti della Società.
La suddetta relazione deve descrivere i procedimenti effettuati per il test del disaster recovery e deve evidenziare gli eventuali discostamenti dal corretto andamento delle procedure.

Si procede alla descrizione nel dettaglio delle fasi del test di disaster recovery:

SCENARIO A: PERDITA SITO PRIMARIO
La simulazione consiste in:

- interruzione della sincronizzazione dello storage primario e riallineamento dei dati dello storage secondario rispetto a quanto contenuto nel cloud;
- procedure di collegamento al cloud (sul sito di DR);
- procedura di avvio del singolo servizio o dei servizi;
- procedure di ripristino della soluzione di disaster recovery.

SCENARIO B: INTERRUZIONE CORRENTE ELETTRICA E COLLEGAMENTO INTERNET
La simulazione consiste in:

- attivazione dei pc portatili di emergenza;
- attivazione del servizio telefonico tramite utilizzo di cellulari;
- collegamento internet UMTS tramite utilizzo di router portatili;
- procedure di ripristino della soluzione di disaster recovery.

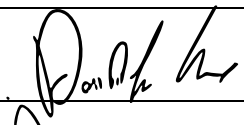
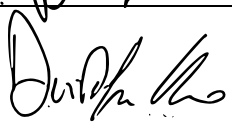
SCENARIO C: DATA RECOVERY
La simulazione della perdita dei dati, consiste in:

- interruzione della sincronizzazione in cloud e del riallineamento dei dati effettuate presso la sede di DR;
- procedure di collegamento al cloud;
- procedure di recupero o di acquisizione di nuove apparecchiature elettroniche se necessario;
- procedure di ripristino della soluzione di disaster recovery.

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato

2.8 Formazione sul Piano BC e DR

La Società provvede all'erogazione di formazione a favore degli addetti al servizio interessato dal presente Piano, a cadenza annuale e comunque ogniqualvolta lo stesso sia modificato.
La formazione è organizzata e svolta a cura del RSIT.

Luogo e Data	**Bari, 24 Luglio 2024**
Firma della Direzione Generale	
Firma del Responsabile SGI per accettazione	

Questo documento è di proprietà della Edilizia e Tecnologia S.r.l. Unipersonale – Strada Privata detta della Marina Trav. 32/A, n. 15, 70126 - Bari - P.Iva 08025530729
Vietato ogni utilizzo non autorizzato