FONDO PENSIONE MEDICI

iscritto n. 1337 alla Sezione I dell'Albo tenuto dalla Covip

Fondo Pensione Preesistente

SITI WEB, TECNOLOGIE INFORMATICHE E RAPPORTI CON GLI ADERENTI

(Piano strategico sulle tecnologie dell'informazione e della comunicazione, sistema informativo del Fondo Pensione e i presidi di sicurezza informatici adottati)

Approvato nella seduta del CdA	**12/05/2021**
Inviato a COVIP	**Non soggetto a invio (integrato nel Documento della Governance)**
Pubblicato sul sito internet	**02/12/2023**
Soggetto a revisione annuale	**02/12/2023**

INDICE

1.	PREMESSA	pag. 2
2.	ARTICOLAZIONE DEL SISTEMA INFORMATICO	pag. 2
3.	PRESIDI DI SICUREZZA	pag. 3
4.	PASSWORD POLICY: la gestione delle credenziali di accesso	pag. 3
4.1	Campo di applicazione	
5.	RESPONSABILITA' DEGLI IMPIEGATI	pag. 4
6.	RACCOMANDAZIONI	pag. 5
7.	PRESIDI DI SICUREZZA INFORMATICI ADOTTATI DAL SERVICE AMMINISTRATIVO PREVINET – BUSINESS CONTINUITY PLAN	
8.	OBIETTIVI DEL SISTEMA INFORMATIVO E DEI PRESIDI DI SICUREZZA INFORMATICA	pag. 22

1. PREMESSA

L'informatica è una delle modalità operative al servizio di tante necessità, in ogni ambito della vita lavorativa, che ha amplificato lo sviluppo della conoscenza, del progresso, della velocità di divulgazione delle notizie ma, di contro, ha posto in essere problematiche non da poco sul rischio che i sistemi possono incorrere ove non si pongono a presidio di sicurezza attività e normative atte ad arginare il non corretto utilizzo, la scarsa propensione alla sicurezza ed archiviazione dei dati, alla intrusione fraudolente nei sistemi informatici.
Tutto ciò può esporre, qualsiasi settore produttivo e tra questi, quindi, il Fondo, a rischi di tipo patrimoniale creando problemi di immagine, di sicurezza dei dati e di integrità e riservatezza delle informazioni.
E' consequenziale che tale criticità possa determinare aspetti sanzionatori da parte degli organismi di controllo e della COVIP in particolare.
Il Fondo adotta, quindi, rigide procedure e regolamenti interni (*già illustrati nel Codice Etico e nel Documento sui Conflitti di interesse adottati*) sull'importanza del corretto utilizzo dei sistemi informatici, sulla protezione dei dati, sulle modalità di accesso, sulla riservatezza da seguire uniformando il comportamento del personale deputato a tali compiti nonché il corretto utilizzo del sistema informatico.
La maggior parte delle informazioni aziendali sono gestite attraverso l'impiego di strumentazione informatica che a sua volta deve essere utilizzata secondo modalità in grado di garantire la sicurezza dei dati trattati.
Il corretto impiego di tali presidi informativi è parte integrante della mission del Fondo ed ogni operatore (interno o in funzione di esternalizzazione) è tenuto ad adottare, nell'ambito delle proprie attività, tutte le misure di sicurezza atte a prevenire la possibilità di un utilizzo non congruo alle finalità del Fondo.

2. ARTICOLAZIONE DEL SISTEMA INFORMATICO

Il Fondo, utilizzando i sistemi informativi di cui si è dotato, ha adottato misure appropriate atte a garantire la continuità e la regolarità dello svolgimento della propria attività (salvaguardia all'accesso mediante password dedicate e rilasciate in funzione consultiva o dispositiva in funzione dei compiti svolti) sia tra il personale della sede del Fondo che tra coloro che, in attività di processi prestati in outsourcing, possono avere accessi ai dati informatici settorializzati (per le parti di loro competenza ed attività) per il corretto funzionamento della macchina amministrativa del Fondo (ciclo attivo e ciclo passivo).
Pertanto le varie aree informatiche sono state configurate al fine di garantire livelli progressivi di accesso e sicurezza onde permettere ai beneficiari di essere a conoscenza dei flussi contributivi, alla tipologia delle prestazioni fornite, alle caratteristiche organizzative dei soggetti tenuti alla contribuzione.
Peraltro il complesso mondo informatico è un valido aiuto messo a disposizione dell'organo esecutivo e di controllo, per lo svolgimento delle proprie funzioni di direzione e controllo e di tutte quelle attività che restano direttamente affidate alle proprie strutture interne, onde poter gestire al meglio il controllo delle attività demandate, dei processi deputati al corretto svolgimento delle procedure e, quindi , attraverso i sistemi informativi dare un massiccio contributo alla gestione del rischio.

3. PRESIDI DI SICUREZZA

Il sistema informatico è provvisto di idonei presidi di sicurezza volti a tutelare l'integrità del patrimonio informativo, con particolare riferimento alla gestione delle abilitazioni per l'inserimento dei dati nonché all'esistenza di apposite procedure di ripristino delle condizioni antecedenti un evento accidentale (sistemi e punto di ripristino, di back-up e di recovery, etc.). Condizione preliminare osservata è quello di utilizzare pc e software acquistati sul mercato ufficiale ed aventi requisiti di rispetto della normativa CEI.
L'articolazione dei presidi del sistema informatico garantisce, inoltre, il rispetto della normativa vigente in materia di privacy e di tenuta e gestione di banche dati.
In tale ambito il Fondo prevede specifiche misure di sicurezza informatica relativamente ai seguenti aspetti:

- Sistemi di back-up dei dati eseguiti in duplice copia. Esiste comunque un archivio cartaceo di tutte le attività svolte dal Fondo che successivamente ne prevedono il loro inserimento sui sistemi computerizzati;
- Sicurezza dell'infrastruttura di rete: la dotazione informatica del Fondo dispone di un sistema firewall capace di proteggere la rete informatica da virus e da eventuali intrusioni da parte di hacker. Tutte le postazioni di lavoro sono dotate di specifici programmi antivirus. L'infrastruttura in dotazione al Fondo è caratterizzata da un filtro anti-spam che blocca immediatamente mail contenenti virus e maleware;
- Disaster recovery: per poter far fronte in modo opportuno ad eventuali emergenze informatiche. Il piano di disaster recovery stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino la indisponibilità dei centri di elaborazione mediante reinstallazione dei dati partendo da un punto di ripristino temporale.

Tale funzionalità è anche stata richiesta a Previnet, che ha elaborato ed ha in essere un proprio piano di disaster recovery, successivamente acquisito da parte del Fondo nelle sue varie articolazioni, facente parte integrante della Politica della gestione del rischio.
Ciò permette l'attuazione di un piano di emergenza di continuità operativa (contingency plan) per la gestione di eventuali criticità:

a. Interruzione della continuità operativa;
b. Immediato avviso agli organi di Governo del Fondo;
c. Immediato avviso alla commissione di Controllo Interno;
d. Immediato avviso alle attività esternalizzate che hanno accesso ai dati service esterno, banca fiduciaria, responsabile della privacy;
e. Valutazione delle cause di interruzione mediante analisi dei sistemi di allerta antivirus;
f. Valutazione dei danni (anche con verifiche incrociate sui sistemi di archiviazione di backup) di eventuale assenza di aree di archiviazione o malfunzionamento di procedure;
g. Blocco di tutte le password di accesso al sistema informatico (per gli addetti ai lavori) e rilascio di nuove credenziali.

4. PASSWORD POLICY: La gestione delle credenziali di accesso

La protezione delle credenziali di accesso rappresenta uno dei principi fondamentali della sicurezza delle informazioni, in particolare la creazione e la gestione delle password che costituiscono la principale contromisura agli accessi non autorizzati.
Visto quanto previsto dall'attuale codice in materia di protezione dei dati personali – D.Lgs. 196/03 – successivamente ripreso dal nuovo regolamento europeo in vigore dal 24/05/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali – GDPR UE 2016/679

– occorre definire misure di protezione adeguate ed idonee per il trattamento e la tutela dei dati personali degli utenti.
Il presente documento ha lo scopo di definire una procedura – la password policy del Fondo Pensione Medici – che stabilisca i criteri per la creazione, l'utilizzo, la conservazione e la gestione delle credenziali di autenticazione fornite al personale del Fondo Pensione Medici per l'accesso ai computer loro assegnatigli.
Il sistema di autenticazione basato sulle credenziali di accesso consiste in un codice di identificazione dell'impiegato ("username" o "ID utente"), associato ad una parola chiave riservata ("password") conosciuta esclusivamente dal dipendente. I due elementi, uniti insieme, costituiscono la credenziale di accesso ("account" o "utenza") così come definito dalla normativa vigente in tema di dati personali.

4.1 Campo di applicazione

La password policy si applica a tutti i servizi informatici centrali, gestionali ed applicativi, compresi quelli web, alle postazioni di lavoro, alla rete wi-fi, al servizio di posta elettronica e a tutte le applicazioni e risorse informatiche presenti nel Fondo che prevedono un sistema di autenticazione per l'accesso.

5. RESPONSABILITÀ DEGLI IMPIEGATI

Gli utenti si impegnano a rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso di seguito indicati.
Una volta in possesso delle credenziali, i dipendenti dovranno cambiare la password, rispettando i criteri di seguito descritti ed evitando combinazioni facili da identificare. Gli stessi, dovranno scegliere password univoche e ragionevolmente complesse, così da renderne difficile l'individuazione da parte di terzi.
La password è strettamente personale e non deve essere rivelata né condivisa con altre persone all'interno del Fondo Pensione Medici.
Inoltre, gli utenti devono prestare attenzione a non fornire le proprie credenziali di accesso, rispondere ad e-mail sospette e/o cliccare sui link durante la navigazione web (o nella mail), al fine di contrastare possibili frodi informatiche (come il phishing, lo spear phishing, il furto d'identità, ecc.).
Ogni impiegato è responsabile di tutte le azioni e le funzioni svolte dal suo account. Qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi, l'utente dovrà cambiare immediatamente la password.
Per la conservazione sicura delle credenziali di accesso è consigliabile usare un software di gestione delle password (es. KeePass, LastPass, ecc.) evitando di memorizzarle su fogli di carta, documenti cartacei e file conservati all'interno della postazione di lavoro; tali software permettono anche di automatizzare il processo di login alle varie applicazioni usate.
Qualora l'utenza venga bloccata a seguito della scadenza della password o l'utente si dimentichi la password o si renda necessaria la modifica della password per altre motivazioni, si dovranno utilizzare i servizi self-service di reimpostazione o di cambio password messi a disposizione dal sistema, oppure contattare la segreteria del Fondo. Tale procedura è applicata anche all'area riservata degli aderenti.

6. RACCOMANDAZIONI

Nei limiti tecnici consentiti dai sistemi, la password:

1) deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui il sistema non lo dovesse prevedere, di lunghezza pari al massimo consentito;
2) deve essere obbligatoriamente cambiata al primo utilizzo e successivamente almeno ogni 6 (sei) mesi;
3) deve contenere, ove possibile, almeno 3 caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali;
4) deve essere sempre diversa da almeno le ultime 4 precedentemente utilizzate;
5) non deve presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti;
6) deve essere nota esclusivamente all'utilizzatore e non può essere assegnata e/o comunicata ad altri;
7) non deve contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti;
8) non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere) o che si riferiscano ad informazioni personali;
9) non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet.

Ove tecnicamente possibile, i requisiti di cui ai punti da 1) a 5) devono essere imposti da meccanismi automatici del sistema. Tale procedura è applicata anche all'area riservata degli aderenti.

7. PRESIDI DI SICUREZZA INFORMATICI ADOTTATI DAL SERVICE AMMINISTRATIVO PREVINET – BUSINESS CONTINUITY PLAN (VEDI ALLEGATO)

8. OBIETTIVI DEL SISTEMA INFORMATIVO E DEI PRESIDI DI SICUREZZA INFORMATICA

Il sistema informativo, composto principalmente dal sito internet del Fondo, rappresenta, di fatto, l'interfaccia con la platea degli aderenti iscritti o di quelli potenziali aderenti futuri, con le fonti Istitutive, con le Aziende che partecipano al Fondo Pensione Medici, con l'organo di vigilanza (COVIP), con le strutture esterne che svolgono attività esternalizzata.
Al fine di essere esaustiva nei contenuti che deve illustrare la home page del sito del Fondo Pensione Medici e le varie articolazioni che da questa, attraverso vari link, è possibile raggiungere, deve contenere tutti gli obblighi informativi e comunicazioni che la normativa (D.Lgs. 252/05, successive modifiche fino alla IORP II) esplicita e fornisce in materia di informativa ai potenziali aderenti, agli aderenti e ai beneficiari. Pertanto il sito WEB contiene informazioni consultabili in aria pubblica, in area riservata ed in area dedicata alle Aziende. Ognuno di tale settore ha modalità di accesso univoche e disciplinate da un livello di differente accesso e controllo (nullo sull'area pubblica, con credenziali sulle aree riservate).
Tutto il sito, nei vari settori consultabili in pubblica e/o in area con accesso mediante credenziali dedicate e riservate, contiene le seguenti informazioni:

- informazioni generali sulla forma pensionistica complementare, che il Fondo mette a disposizione degli aderenti e dei beneficiari attraverso lo Statuto e la Nota Informativa, nonché attraverso la "Comunicazione periodica";
- informazioni ai potenziali aderenti che il Fondo ha previsto all'interno della Nota Informativa e anche nella sezione "Notizie Sintetiche per l'Aderente";

• informazioni periodiche agli aderenti che il Fondo ha previsto all'interno della "Comunicazione periodica - Prospetto delle prestazioni pensionistiche", in cui vengono anche fornite informazioni circa le proiezioni delle prestazioni pensionistiche basate sull'età di pensionamento. Tale ultima funzione usufruisce anche di un motore di calcolo che può essere confrontato con quello presente sul sito dell'INPS con analoga funzione;
• informazioni agli aderenti durante la fase di prepensionamento che il Fondo fornisce all'aderente, almeno tre anni prima dell'età di pensionamento (o anche successivamente se richieste) in merito alle opzioni di erogazione della prestazione pensionistica maturata;
• informazioni ai beneficiari durante la fase di erogazione delle rendite attraverso comunicazioni periodiche dedicate.

ATTENZIONE: l'adesione al Fondo Pensione Medici non è consentita mediante modalità web in quanto, essendo il Fondo di natura negoziale è riservata a coloro i quali hanno rapporto di dipendenza (CCNL Aris Anmirs). La procedura di assunzione è base di riferimento indispensabile per poter accedere all'iscrizione del Fondo Pensione Medici mediante scheda di adesione. Tutte le informazioni raccolte dagli uffici del personale delle strutture ospedaliere censite ed aderenti al Fondo Pensione Medici sono indispensabili e base di riferimento per una corretta procedura informatizzata che dovrà necessariamente collegare l'assunzione/adesione agli uffici della segreteria del Fondo e, di conseguenza, all'anagrafica da creare presso il service amministrativo (attualmente Previnet).

Sul sito WEB, nel rispetto del requisito di trasparenza e di un chiaro e corretto rapporto con gli iscritti, il Fondo, come previsto dal D.Lgs. 252/05, pubblica gli specifici documenti o informazioni di seguito riportati:

- il documento sul sistema di governo
- le informazioni essenziali e pertinenti relative alla politica di remunerazione
- il documento sulla politica di investimento
- i bilanci e le relative relazioni
- Il glossario dei termini tecnici più utilizzati.

Nella sezione dedicata ai singoli aderenti (area riservata) il Fondo mette a disposizione:

- informazioni relative alla contribuzione versata e alla posizione individuale maturata in corso d'anno, e di consentire agli interessati il controllo della correttezza dei versamenti;
- facilita l'interlocuzione tra lo stesso e gli iscritti, prevedendo la possibilità di compilare moduli o schede on-line per l'invio delle richieste di prestazioni o di trasferimento.

Tali funzioni saranno implementate nel rispetto della direttiva europea IORP II e delle nuove regole in materia di trasparenza in ottemperanza a quanto emanato da COVIP con il provvedimento del 22 dicembre 2020.

Infine, il Fondo si è dotato di un indirizzo di posta elettronica certificata necessaria sia per la gestione dei rapporti con gli iscritti (per le richieste volte all'esercizio di prerogative individuali, quali trasferimento, riscatto, etc.), sia per gestire l'interlocuzione con la COVIP.

<u>I responsabili del sistema informatico sono:</u>

- L'amministratore di sistema riconosciuto nella società ITLAb360 s.r.l.s. con sede in Piazza Vittorio Malatesta 8 – Roma;
- il Presidente pro-tempore;
- l'impiegato Carmelo Daniele;

Funzioni operative informatiche:

- **Le password dispositive** sono in possesso del Presidente pro-tempore e, in sua assenza o impedimento, del Vice-Presidente.
- Gli impiegati Giulia Paolone e Carmelo Daniele hanno accesso a tutte le funzioni delle procedure informatiche ad esclusione delle funzioni derivanti dall'utilizzo delle password dispositive (prerogativa del Presidente e Vice-Presidente).

Operatività sul sito WEB

L'impiegato Carmelo Daniele è il solo abilitato a variare il contenuto del sito web del Fondo Pensione Medici ed apportarne modifiche in ottemperanza a disposizioni di legge e/o raccomandazioni COVIP o ogni qual volta si rende necessario, su delibera del CdA o determinazione del Presidente e del Direttore Generale (comunicazione scritta da archiviare).

Business Continuity Plan

(Procedura)

Italiano

	Data	*Cognome Nome*	*Ruolo / Area*
Creazione/Modifica:	28.04.2023	-	Security Governance
Approvazione:	17.05.2023	-	Referente del Comitato per la gestione della Business Continuity
Controllo:	08.05.2023	-	Comitato per la gestione della Business Continuity Funzioni di controllo

	Tipo	*Codice*	*Revisione*
Documento:	Procedura	PRC_002	13

STORIA DELLE REVISIONI

Revisione	*Data*	*Descrizione Della Modifica*
1	03/2011	Prima emissione
2	04/2012	Revisione annuale
3	11/2013	Revisione annuale
4	10/2014	Revisione annuale
5	11/2015	Revisione annuale
6	12/2016	Revisione annuale
7	10/2017	Revisione annuale
8	10/2018	Revisione annuale e adeguamenti
9	07/2019	Revisione annuale e adeguamenti
10	05/2020	Revisione annuale e adeguamenti
11	07/2021	Revisione annuale e adeguamenti: - Integrazione della Lista di distribuzione; - Ridenominazione del Comitato di Emergenza in Comitato per la gestione della Business Continuity e Aggiornamento della composizione; - Estensione del perimetro dei processi analizzati
12	09/2022	Revisione annuale e adeguamenti - Aggiornamento lista di distribuzione

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

		- Aggiornamento composizione del comitato per la gestione della Business Continuity. - Revisione delle modalità di test degli scenari
13	05/2023	Aggiunta soluzione IT “near business continuity”

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

INDICE

1 Generalità del documento 4
1.1 Scopo e campo di applicazione 4
1.2 Definizioni ed abbreviazioni 6
2 Caratteristiche del piano 7
2.1 Copertura del piano 7
2.2 Certificazioni e Attestazioni 8
3 Ruoli e responsabilità nella gestione della continuità operativa 10
3.1 Comitato per la gestione della Business Continuity 10
3.2 Composizione del Comitato 11
4 Notifiche relative all'attivazione del piano 12
5 Tempi di Ripristino in caso di Near Business Continuity 13
6 Tempi di Ripristino in caso di DR 14
7 Scenari di continuità operativa e misure operative 15
7.1 Scenario (A) – Inaccessibilità o indisponibilità dei locali 15
7.2 Scenario (B) – Indisponibilità del personale 16
7.3 Scenario (C) – Indisponibilità dei sub–fornitori 16
7.4 Scenario (D) – Indisponibilità dei sistemi informativi critici 17
7.5 Scenario (E) – Indisponibilità della documentazione fondamentale (dati e documenti critici) 18
7.6 Scenario (F) – Interruzione del funzionamento delle infrastrutture 18
7.7 Scenario (G) – Indisponibilità di dotazioni specifiche 20
8 Formazione e test di verifica 21
9 Registrazione e archiviazione dei documenti 22
10 Revisione 23
11 Allegati 24
11.1 Allegato 1 al Business Continuity Plan "PNET – BCDR – Piano dei test" 25

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

1 Generalità del documento

1.1 Scopo e campo di applicazione

Per rafforzare l'impegno a garantire adeguati livelli di continuità operativa, Previnet S.p.A. si è dotata di un piano di continuità operativa o business continuity plan (BCP) come misura preventiva, di un servizio di "Near Business Continuity" e di un Disaster Recovery Plan (DRP) come misure protettive, al fine di predisporre procedure atte alla gestione di situazioni di crisi conseguenti a incidenti di portata settoriale ovvero a eventi avversi o minacce che colpiscano la società, col fine di ridurre al minimo le conseguenze o gli impatti negativi di eventi catastrofici e non catastrofici che impediscono la normale erogazione dei servizi.

In particolare, sono gestiti da Previnet i seguenti scenari[1]:

a) indisponibilità o inaccessibilità dei locali;
b) indisponibilità del personale;
c) indisponibilità dei sub-fornitori;
d) indisponibilità dei sistemi informativi critici;
e) indisponibilità della documentazione fondamentale (dati e documenti critici);
f) interruzione del funzionamento delle infrastrutture;
g) indisponibilità di dotazioni specifiche.

Per la redazione del presente piano attraverso lo strumento di Business Impact Analysis o BIA, sono stati identificati i processi critici di cui deve essere garantito il funzionamento anche nel periodi di crisi, gli scenari di rischio e gli impatti (economici, normativi e reputazionali) associati alle diverse possibili fasce temporali di indisponibilità del Processo.

Sono inoltre state analizzate le procedure informatiche di supporto, il personale addetto, le strutture logistiche interessate, le infrastrutture tecnologiche e di comunicazione utilizzate per stabilire le misure tecniche e organizzative previste per fronteggiare gli eventi che provocano l'indisponibilità dei centri di elaborazione dei dati e consentire il funzionamento delle procedure informatiche rilevanti nei siti alternativi a quello di produzione (Near Business Continuity e Disaster Recovery Plan).

[1] Come best practice, Previnet ha considerato Circolare Banca d'Italia n. 285 del 17/12/2013 e successivi aggiornamenti (Parte I, Titolo IV, cap. 3, 4 e 5), Art.21 Regolamento Delegato (UE) 565/2017, Art.19 del Regolamento di attuazione degli articoli 4-undecies e 6, comma 1, lettere b) e c-bis) del TUF, Codice delle Assicurazioni Private, art. 30, Regolamento IVASS n. 38/2018, art. 16 c.2 e), art. 19, cc. 5 e 6, Atti Delegati art. 258, paragrafo 3; Art. 4-bis, comma 6 del D. Lgs. n. 252/2005 come integrato dal D. Lgs. n. 147/2018, in attuazione della direttiva (UE) 2016/2341 con delibera COVIP 29 luglio 2020.

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

Le responsabilità delle fasi del processo di gestione del presente documento sono così declinate:

Redazione	Validazione	Approvazione	Divulgazione	Archiviazione	Controllo
Security Governance (Funzioni di Controllo Interno)	Comitato per la gestione della Business Continuity	Referente del Comitato per la gestione della Business Continuity	Funzioni aziendali coinvolte (HR e Compliance)	Funzioni di Controllo Interno	Comitato per la gestione della Business Continuity (Funzioni di Controllo Interno)

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

1.2 Definizioni ed abbreviazioni

Business continuity / Continuità operativa	Capacità di un'organizzazione di continuare a fornire prodotti e servizi a un livello accettabile e predefinito, dopo un evento disastroso.
Business continuity plan / Piano di continuità operativa / (BCP)	Documento che fornisce una guida per affrontare una situazione di disastro, al fine di ripristinare e mantenere il funzionamento dei processi critici, secondo le priorità stabilite nella BIA di ogni unità organizzativa.
Business impact analysis / Analisi di impatto sull'operatività (BIA)	Processo utilizzato dall'organizzazione per analizzare l'effetto che un'interruzione di servizio può avere sulle attività che supportano la produzione dei prodotti o dei servizi che ne costituiscono il business.
Risk Assessment	Analisi e valutazione degli scenari di rischi e degli impatti che possono verificarsi nel progredire delle fasce orarie di indisponibilità di ciascun processo in termini di impatto economico, normativo e reputazionale.
Disaster / Disastro	Evento improvviso, non pianificato, con effetto severo o catastrofico sull'operatività, sulle strutture o sulle persone dell'organizzazione.
Disaster Recovery Plan (DRP)	Documento che indica le procedure per ripristinare i sistemi informativi presso una sede alternativa dopo un'emergenza.
Recovery Point Objective (RPO)	Il punto (l'istante nel tempo) al quale le informazioni sono coerenti e possono essere ripristinate per consentire la ripresa delle attività (denominato anche Maximum Data Loss).
Recovery Time Objective (RTO)	Il periodo di tempo entro il quale i servizi erogati devono essere ripristinati dopo l'incidente che ha generato la discontinuità.
Service Level Agreement (SLA)	Accordo sul livello del servizio: strumento contrattuale che definisce le metriche di servizio che devono essere rispettate da un fornitore di servizi (provider) nei confronti dei propri clienti/utenti.
PDL	Postazioni di lavoro

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

2 Caratteristiche del piano

2.1 Copertura del piano

Si ricorda che:

- Le misure di contrasto e contenimento individuate devono essere commisurate all'effettivo beneficio, ovvero gli interventi devono arrecare il minor danno possibile agli asset ICT, ai servizi da questi gestiti o ad altri processi di continuità aziendale;

- I danni o i disservizi degli asset ICT, causati dall'intervento o delle misure di contrasto e contenimento, devono comunque essere inferiori a quelli conseguenti dallo scenario verificatosi;

- In nessun caso sono ammesse operazioni tali da comportare, direttamente o indirettamente, una violazione delle politiche di sicurezza in vigore, alle clausole contrattuali o alle vigenti leggi;

- Non sono ammessi interventi che possano arrecare un qualsiasi danno, materiale o morale, a persone fisiche, sia dipendenti che esterni all'Organizzazione;

- La tempistica con la quale devono essere ripristinati i processi operativi viene stimata dai singoli Referenti di processo ed è costituita dai tempi di analisi degli eventi, identificazione dello scenario, decisione delle azioni da intraprendere anche in base ai livelli di servizio concordati con i Clienti, e dalla ripartenza del processo attraverso l'attuazione degli interventi tecnici e organizzativi previsti;

- Durante l'attivazione del BCP, ogni unità aziendale esegue le proprie attività gestionali/ operative/ tecniche, con la miglior diligenza, come da propria Business Impact Analysis;

- Per quanto concerne la strategia di back up, i sistemi informatici e le applicazioni IT critici sono replicati o sottoposti a backup con una frequenza conforme alle esigenze aziendali, verificati tramite test di ripristino per garantire che il backup funzioni correttamente e sottoposti a misure di sicurezza dei backup per i dati a riposo o in transito (ad es. restrizioni all'accesso fisico, transito sicuro, ecc.).
  Previnet possiede almeno tre copie dei dati, conservate su due supporti diversi, di cui uno off-site (regola 3-2-1). Per la terza copia Previnet adotta quale supporto i nastri magnetici, mezzo di archiviazione sicuro per la protezione e la conservazione a lungo termine dei dati.
  Tutti i processi e gli standard adottati per il salvataggio o backup dei dati sono stabiliti nell'apposita procedura interna regolata dal proprio sistema di gestione della sicurezza delle informazioni ISO 27001;

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

- Per le sue applicazioni critiche e sistemiche, Previnet ha realizzato una soluzione a tre siti. Il Centro di Elaborazioni Dati (CED) o sito primario di produzione *"hot site",* localizzato in Via Enrico Forlanini, 24, 31022 Preganziol TV, il sito secondario per la Near Business Continuity o "*warm site*" con replica sincrona dei dati, rappresentato dalla sede di ASCO Tlc S.p.A, IDC Tier III di Santa Lucia di Piave, situato a Via E. Maiorana, 14, Area Insediamenti Produttivi Foresto (TV). Il sito di "Near BC", può essere configurato per essere accessibile in modo totalmente trasparente da parte dei Clienti in caso di indisponibilità del sito primario. Analogamente, Previnet dispone di un sito di DR o "*warm site*" con trasmissione asincrona dei dati o backup. Il DR site o sito alternativo è rappresentato dalla sede di Sintea Servizi Informatici S.r.l., situato in via Perugia 56, Torino, situata a circa 400 km dal sito primario, per garantire un profilo di rischio distinto e impedire che venga colpito dall'evento che ha interessato il sito primario. Il sito di DR può essere utilizzato, in caso di necessità, anche per periodi prolungati ed è già allestito e completo dei dispositivi e infrastrutture da utilizzare in caso di emergenza, dotato di risorse, capacità, funzionalità e personale sufficienti e adeguato a soddisfare le esigenze commerciali e garantire gli SLA con i Clienti. Il sito di DR è immediatamente accessibile al personale della Società per garantire la continuità dei servizi critici qualora il sito primario di elaborazione dei dati divenga indisponibile.

2.2 Certificazioni e Attestazioni

Con l'obiettivo di garantire un adeguato grado di sicurezza, integrità, disponibilità e confidenzialità nel trattamento dei dati gestiti all'interno della propria infrastruttura per conto dei Clienti, Previnet ha conseguito la **certificazione ISO27001** sul proprio sistema di gestione della sicurezza implementato (ISMS) nel seguente ambito "Gestione dell'infrastruttura tecnologica connessa all'erogazione dei servizi della società in ambito finanziario, assicurativo e previdenziale".

L'ISMS di Previnet prevede l'attuazione di procedure e controlli, svolti dal personale aziendale, per il raggiungimento e mantenimento nel tempo degli obiettivi seguenti:

a. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
b. Garantire la sicurezza incorporata come elemento essenziale delle reti, dei sistemi informativi, delle operazioni e degli accessi alle informazioni in modo da prevenire trattamento non autorizzati o realizzati senza i diritti necessari.
c. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

d. Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano consapevolezza della necessità della sicurezza delle informazioni.
e. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
f. Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
g. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
h. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
i. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

Le misure di sicurezza vengono monitorate nel continuo e riviste periodicamente in fase di analisi del rischio per garantire un continuo adeguamento ai cambiamenti del sistema e delle minacce. Il sistema di sicurezza viene sottoposto ad audit annuali dall'ente di certificazione.

In aggiunta, con l'entrata in vigore del Regolamento UE 2016/679 noto come GDPR, i 114 controlli della norma volti ad assicurare riservatezza, integrità e disponibilità delle informazioni, resilienza dei sistemi e recupero in caso di incidente rilevante, sono stati verificati e integrati con specifiche misure per le informazioni di carattere personale, in linea con la norma ISO 29100 e lo standard NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations).

Previnet dal 2019 ottiene annualmente le attestazioni ISAE 3402 (o SOC 1, Type II) e ISAE 3000 (o SOC 2, Type II) sull'intero anno di osservazione. Tali attestazioni sono garanzia terza del grado di adeguatezza e di effettività del sistema di controllo interno adottato da Previnet nell'erogazione di servizi ai propri Clienti. In particolar modo l'attestazione SOC 2 si focalizza sugli aspetti della sicurezza dell'organizzazione, alla disponibilità, all'integrità del trattamento, alla riservatezza e/o alla privacy, alla governance. Il perimetro delle attestazioni SOC è quello dei fondi pensione internazionali e dei prodotti assicurativi.

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

3 Ruoli e responsabilità nella gestione della continuità operativa

Ai fini della definizione del presente piano, Previnet ha definito ruoli e competenze degli organi aziendali e di tutte le risorse coinvolte nella gestione della crisi, assicurando le risorse umane, tecnologiche e finanziarie adeguate.

3.1 Comitato per la gestione della Business Continuity

Il Comitato di Gestione della Business Continuity è l'organismo di vertice nella gestione delle crisi a cui spettano le principali decisioni e la supervisione delle attività delle risorse coinvolte.
Le mansioni principali sono:

- Definizione, approvazione e aggiornamento del piano di continuità operativa in ragione delle esigenze aziendali e degli obiettivi di business, dai risultati delle verifiche effettuate, dall'individuazione di nuovi rischi e minacce;
- Coordinamento della pianificazione dei test periodici delle procedure di continuità e di disaster recovery e valutazione dei risultati ottenuti dai test periodici, in termini di aspettative interne e livelli di servizio con i Clienti e definizione di eventuali misure correttive;
- Valutazione delle situazioni di emergenza e dello scenario realizzato e dichiarazione dello stato di crisi;
- Attivazione del piano di continuità operativa e attività di recovery e controllo del loro svolgimento;
- Regolamento delle comunicazioni verso dipendenti e verso l'esterno;
- Avvio delle attività di rientro e controllo del loro svolgimento;
- In caso di emergenza, attivazione degli addetti alle emergenze come stabilito nel Piano di Emergenza di Previnet;
- Dichiarazione di rientro;
- Riunione con periodicità almeno annuale;
- Assicurare che venga data adeguata comunicazione del piano di continuità ai dipendenti.

Tutte le decisioni del Comitato sono documentate.

Il Comitato può essere attivato da:

- Responsabili delle unità operative;
- Datore di Lavoro.

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

3.2 Composizione del Comitato

Il Comitato per la gestione della Business Continuity è composto dai seguenti componenti:

Funzione	Nome	Contatto
Referente del Comitato	Luca Rizzi (Information Technology)	[redacted]
Amministratore Delegato	Marco Favaretto (Amministratore Delegato)	[redacted]
Componente del comitato	Stefano Fabbro (Finance)	[redacted]
Componente del comitato	Enrico Facchinello (Finance)	[redacted]
Componente del comitato	Antonio Milici (Assicurazioni)	[redacted]
Componente del comitato	Alessio Garbin (Fondi Pensione)	[redacted]
Componente del comitato	Dania Pussini (Fondi Pensione)	[redacted]
Componente del comitato	Martino Braico (Clienti Internazionali)	[redacted]
Componente del comitato	Dejan Malesic (Clienti Internazionali)	[redacted]
Componente del comitato	Silvia Galante (Amministrazione)	[redacted]
Componente del comitato	Annalisa Vivian (Risorse Umane)	[redacted]

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

4 Notifiche relative all'attivazione del piano

Tutte le comunicazioni verso l'interno e, ove necessario, verso l'esterno (clienti, fornitori, collaboratori, media) sono regolate dal Comitato di Gestione della Business Continuity e vengono effettuate in linea a quanto eventualmente previsto nei contratti.

Il contenuto della notifica di attivazione del piano (e relativi aggiornamenti incluso il rientro in condizioni di normalità) sarà quanto strettamente autorizzato e approvato dal Comitato di Gestione della Business Continuity.

È fatto divieto a chiunque non autorizzato di divulgare informazioni non approvate dal Comitato.

Al fine di una tempestiva comunicazione, Previnet attiva lo schema come sotto riportato e dispone delle informazioni di contatto aggiornate dei propri dipendenti e controparti (e-mail e telefono).

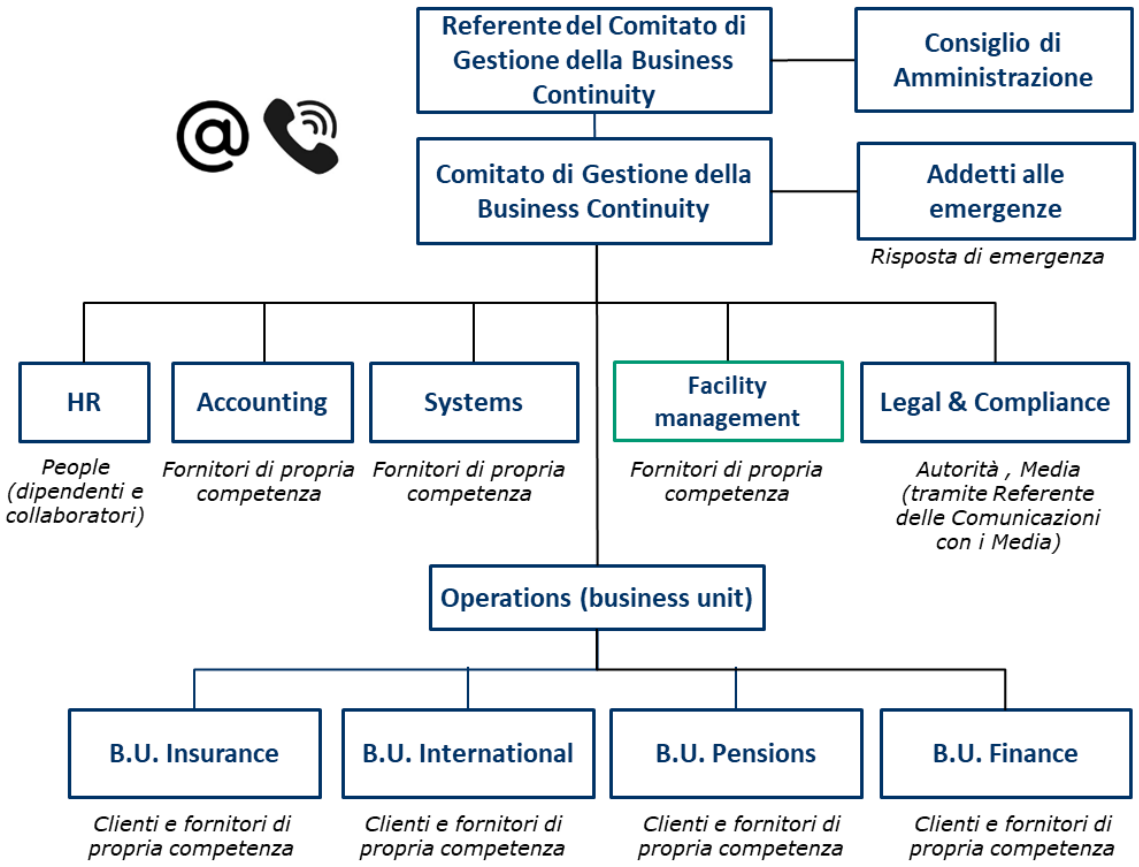

Figura 1: Albero delle notifiche

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

5 Tempi di Ripristino in caso di Near Business Continuity

Con la sigla **RPO** (*Recovery point objective*) si intende il massimo tempo che intercorre tra la produzione di un dato nel sito primario e la sua messa in sicurezza attraverso la replica sincrona dei dati nel sito secondario.

Con la sigla **RTO** (*Recovery Time Objective*), si intende il tempo massimo che intercorre dalla dichiarazione dello stato di crisi fino al ripristino completo dell'infrastruttura aziendale a fronte di un evento disastroso.

Il *Recovery Time Objective* è costituito dai tempi di:

- Analisi degli eventi, individuazione dello scenario e decisione delle azioni da intraprendere (vedi §7);
- Ripartenza del processo, attraverso l'attuazione delle misure tecniche organizzative previste e successiva verifica circa la disponibilità dei servizi senza danni e in condizioni di sicurezza.

Per i processi/clienti aderenti alla "Near Business Continuity, i piani di ripristino consentono il recupero di tutte le operazioni in corso al momento dell'evento di crisi, così da permettere alla controparte di continuare a operare con certezza e di completare le operazioni alla data programmata.

Qualora sia presente l'alternativa di *Near Business Continuty*, di fronte agli scenari di disastro coperti, i livelli di servizi sono indicati nella seguente tabella:

Near Business Continuity	
RPO	~ 0 ore
RTO	~ 15 min

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

6 Tempi di Ripristino in caso di DR

Con la sigla **RPO** (*Recovery point objective*) si intende il massimo tempo che intercorre tra la produzione di un dato nel sito primario e la sua messa in sicurezza attraverso backup nel sito di DR.

Le procedure sono in grado di ripristinare i sistemi con dati non più vecchi di 24 ore dall'evento disastroso.

Con la sigla **RTO** (*Recovery Time Objective*), si intende il tempo massimo che intercorre dalla dichiarazione dello stato di crisi fino al ripristino completo dell'infrastruttura aziendale a fronte di un evento disastroso.

Il *Recovery Time Objective* è costituito dai tempi di:

- Analisi degli eventi, individuazione dello scenario e decisione delle azioni da intraprendere (vedi §7);
- Ripartenza del processo, attraverso l'attuazione delle misure tecniche organizzative previste e successiva verifica circa la disponibilità dei servizi senza danni e in condizioni di sicurezza.

Salvo diversamente indicato nel Contratto tra Previnet e il Cliente, i tempi di ripristino del Sistema Informativo nella sua globalità sono di 72 ore.

In sintesi, salvo diversamente contrattualizzato i livelli di servizi per il *Disaster Recovery* sono indicati nella seguente tabella:

Disaster Recovery	
RPO	24 ore
RTO	72ore

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

7 Scenari di continuità operativa e misure operative

Il Comitato per la gestione della Business Continuity e il Gruppo Operativo di emergenza di Previnet hanno individuato i seguenti scenari di crisi, definendo soluzioni e misure operative da adottare, in base a diversi livelli di gravità identificabili per ogni scenario:

a) Indisponibilità dei locali;
b) Indisponibilità del personale;
c) Indisponibilità dei sub-fornitori;
d) Indisponibilità dei Sistemi informativi critici (procedure informatiche e sistemi IT - SW e HW);
e) Indisponibilità della documentazione fondamentale dati e documenti critici;
f) Interruzione del funzionamento delle infrastrutture;
g) Altro: Indisponibilità dotazioni specifiche.

7.1 Scenario (A) – Inaccessibilità o indisponibilità dei locali

Nello scenario (A), i locali di lavoro sono inaccessibili o indisponibili (totalmente o parzialmente) a causa di evento naturale o umano, ma è garantito il funzionamento delle apparecchiature critiche.

Rientrano in questo scenario ad esempio minacce quali attacchi biologici, chimici, rischio nucleare, atti terroristici/bioterrorismo, incidenti ambientali, eventi metereologici estremi, alluvioni e tempeste blocco totale o parziale dei sistemi di trasporto, pandemie, epidemie/malattie.

In funzione della tipologia di evento che ha causato l'indisponibilità e in base al livello di indisponibilità, Previnet prevede:

Livello di gravità	Descrizione	Soluzione e Misure Operative
1	Inaccessibilità parziale con disponibilità di locali alternativi all'interno del campus e garanzia del funzionamento delle apparecchiature critiche (soluzione interna)	1) [illegible] 2) [illegible] 3) [illegible] §3
2	Inaccessibilità totale con garanzia del funzionamento delle apparecchiature critiche (soluzione interna) (Nota1)	1) [illegible] 2) [illegible] (100%): [illegible] 3) [illegible]

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

		[illegible]
3	Inaccessibilità totale con garanzia del funzionamento delle apparecchiature critiche (soluzione esterna)	[illegible]

(Nota 1): se l'inaccessibilità totale della sede è conseguenza di un evento catastrofico, potranno verificarsi contemporaneamente lo scenario A e D (Disaster recovery).

7.2 Scenario (B) – Indisponibilità del personale

Nello scenario (B), si rileva una indisponibilità di personale aziendale essenziale (operativo/gestionale e informatico). Questo scenario prevede l'attivazione al superamento della soglia del 50% di indisponibilità del personale. I casi che non determinano il superamento della soglia di attivazione non si considerano di reale emergenza.
In funzione della tipologia di evento che ha causato l'indisponibilità e in base al livello di indisponibilità, Previnet prevede:

Livello di gravità	Descrizione	Soluzione e Misure Operative
1	Indisponibilità inferiore al 50% del personale di una stessa unità organizzativa (soluzione interna)	1) [illegible]
2	Indisponibilità superiore al 50% del personale di una stessa unità organizzativa (soluzione interna)	1) [illegible] 2) [illegible] 3) [illegible]
3	Indisponibilità superiore al 50% del personale di una stessa unità organizzativa (soluzione esterna)	[illegible]

7.3 Scenario (C) – Indisponibilità dei sub–fornitori

Nello scenario (C) si verifica l'indisponibilità dei sub-fornitori che erogano servizi non bloccanti per l'esecuzione delle attività in capo a Previnet quali data entry, gestione documentale (Digitalizzazione, fase istruttoria, archiviazione sostitutiva), Outbound call, intermediario abilitato incaricato delle trasmissioni dei flussi all'Agenzia delle Entrate, sicurezza fisica e custodia delle sedi.

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

In funzione della tipologia di evento che ha causato l'indisponibilità e in base al livello di indisponibilità, Previnet prevede:

Livello di gravità	Descrizione	Soluzione e Misure Operative
1	Indisponibilità temporanee rispetto agli SLA concordati con i sub-fornitori (disservizi) (soluzione esterna)	1) [illegible]
2	Indisponibilità prolungate rispetto agli SLA concordati con i sub-fornitori (soluzione esterna)	1) [illegible] 2) [illegible] 3) [illegible] §3
3	Indisponibilità prolungate rispetto agli SLA concordati con i sub-fornitori (soluzione interna)	1) [illegible] 2) [illegible] 3) [illegible] 4) [illegible] §3

7.4 Scenario (D) – Indisponibilità dei sistemi informativi critici

Nello scenario (D), sono indisponibili i sistemi informativi critici dal punto di vista fisico e/o logico (ad esempio per un disservizio massivo con conseguente k.o. di tutti i sistemi), a causa di un evento naturale o umano.

In funzione della tipologia di evento che ha causato l'indisponibilità e in base al livello di indisponibilità, Previnet prevede:

Livello di gravità	Descrizione	Soluzione e Misure Operative
1	Casi di malfunzionamenti localizzati non bloccanti (soluzione interna)	1) [illegible]
2	Indisponibilità parziale (ad esempio un guasto localizzato ad una sola macchina di produzione) (soluzione interna)	1) [illegible]
3	Indisponibilità parziale o totale che non consente il ripristino entro gli SLA concordati (fisica e/o logica) (soluzione interna/esterna)	1) [illegible]

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

		2) [illegible] 3) [illegible] §3

7.5 Scenario (E) – Indisponibilità della documentazione fondamentale (dati e documenti critici)

Lo scenario (E) include gli eventi di effetto alterativo o distruttivo parziale o totale di dati e documenti critici, conseguenti a incidenti di sicurezza, infezione da malware o ransomware e/o cancellazione accidentale.

In funzione della tipologia di evento che ha causato l'indisponibilità e in base al livello di indisponibilità, Previnet prevede:

Livello di gravità	Descrizione	Soluzione e Misure Operative
1	Alterazione o perdita dei dati informatici e cartacei presenti in forma digitale	1) [illegible] 2) [illegible] 3) [illegible] 4) [illegible] 5) [illegible]
2	Alterazione o perdita dei dati cartacei non presenti in forma digitale	1) [illegible] 2) [illegible] 3) [illegible]

7.6 Scenario (F) – Interruzione del funzionamento delle infrastrutture

Lo scenario (F) si realizza in caso di interruzione del funzionamento di una o più infrastrutture necessarie all'erogazione dei servizi di Previnet, tra cui energia elettrica, servizio idrico (rete idrica), climatizzazione, reti di telecomunicazioni (dati e fonia fissa), reti interbancarie, mercati finanziari. In ogni caso, viene contattato il provider di riferimento e identificate le strutture coinvolte, la gravità dell'interruzione e la durata stimata dal fornitore.

In funzione della tipologia di evento che ha causato l'indisponibilità e in base al livello di indisponibilità, Previnet prevede:

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

Livello di gravità	Descrizione	Soluzione e Misure Operative
1	Interruzione / indisponibilità temporanea dell'infrastruttura che non pregiudica l'erogazione dei servizi secondo gli SLA concordati	1) [illegible]: - [illegible] - [illegible] - [illegible]; - [illegible] 40 [illegible]); - [illegible]; 2) [illegible]; 3) [illegible].
2	Interruzione / indisponibilità prolungata dell'infrastruttura o comunque che pregiudica l'erogazione dei servizi secondo gli SLA concordati	1) [illegible]: - [illegible]; - [illegible]; - [illegible]; - [illegible]; - [illegible]; 2) [illegible] §3; 3) [illegible]; 4) [illegible]; 5) [illegible].

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

7.7 Scenario (G) – Indisponibilità di dotazioni specifiche

Lo scenario (G) include l'indisponibilità contemporanea delle postazioni di lavoro, quali dotazioni specifiche dei dipendenti.

In funzione della tipologia di evento che ha causato l'indisponibilità e in base al livello di indisponibilità, Previnet prevede:

Livello di gravità	Descrizione	Soluzione e Misure Operative
1	Indisponibilità delle postazioni di lavoro fino al 10% (soluzione interna)	1) [illegible] 2) [illegible]
2	Indisponibilità delle postazioni di lavoro oltre al 10% (soluzione interna)	1) [illegible] 2) [illegible]
3	Indisponibilità delle postazioni di lavoro oltre al 10% (soluzione esterna)	1) [illegible]

Previnet non ha ritenuto necessario prevedere la disponibilità di postazioni di lavoro ridondate al 100%.

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

8 Formazione e test di verifica

La Società si impegna ad erogare una formazione continua sul contenuto del presente Piano.

Il piano di continuità operativa viene regolarmente testato; i tempi e le modalità di verifica sono differenti a seconda degli scenari (per ulteriori dettagli vedasi Allegato “PNET – BCDR – Piano dei test”).

I test sono eseguiti dal personale normalmente incaricato a svolgere i servizi e le relative attività.

Il personale coinvolto viene addestrato sulle misure di Business Continuity e partecipa alle sessioni di verifica delle misure di continuità operativa.

I risultati delle verifiche vengono documentati, opportunamente archiviati e resi disponibili al Comitato per la gestione della Business Continuity; eventuali punti di miglioramento/inefficienze messe in luce dai test vengono analizzate e, ove necessario, riportate a modifica del piano di continuità.

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

9 Registrazione e archiviazione dei documenti

La documentazione afferente il presente Business Continuity Plan è archiviata nella piattaforma aziendale *Seafile* raggiungibile all'URL: https://pbox.previnet.it/.

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

10 Revisione

La revisione del presente documento è a cura del Comitato per la gestione della Business Continuity, su base annuale.

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

11 Allegati

Descrizione documento	Allegato
Allegato 1 - PNET – BCDR – Piano dei test	Vedasi 11.1
Allegato 2 - PNET – BC – Testbook	BC_Testbook_template_2022.xlsx
Allegato 3 – PNET – DR – Testbook	DR_testbook_template_2022.xlsx

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

11.1 Allegato 1 al Business Continuity Plan "PNET – BCDR – Piano dei test"

Scenario	Modalità di verifica	Owner	Periodicità di test
A. Indisponibilità dei locali	**A1.** Parziale: spostamento di alcune PDL e/o utilizzo di PDL di altre aree, avviso all'ufficio sistemi e al fornitore per le attività di Facility Management (RBRE) per lo spostamento delle PDL	Ufficio Sistemi / RBRE / Unità organizzative	Biennale
	A2. Totale: verifica del corretto funzionamento e accesso alla postazione di lavoro da remoto	Ufficio Sistemi	Biennale
B. Indisponibilità del personale	**B1.** Simulazione dell'indisponibilità di più del 50% del personale, utilizzo del back up e verifica dell'esecuzione delle attività giornaliere nel rispetto degli SLA condivisi con i clienti (campione)	Unità organizzative	Annuale
C. Indisponibilità dei servizi di sub-fornitori	**C1.** Simulazione della indisponibilità di alcuni sub-fornitori (processi critici) e internalizzazione delle attività, verificando il rispetto degli SLA condivisi con i clienti (campione)	Unità organizzative	Biennale
	C2. Simulazione della indisponibilità di alcuni sub-fornitori (processi critici) e utilizzo del sub-fornitore di back up, verificando il rispetto degli SLA condivisi con i clienti (campione)	Unità organizzative	Biennale
D. Indisponibilità dei Sistemi informativi critici	**D1.** Test di alta affidabilità secondo il piano dei test infrastrutturali previsti dal Sistema di Gestione certificato ISO 27001	Ufficio Sistemi	Annuale
	D2. Simulazione dell'indisponibilità dei sistemi informativi critici mediante: **D2.1**. Ripristino presso il sito di DR di una porzione dei sistemi, utilizzando un backup dei giorni precedenti al fine di simulare l'operatività giornaliera, con riferimento ai processi definiti critici nelle BIA delle unità organizzative, e verifica del rispetto del RTO condiviso con i Clienti. Tale test viene effettuato da remoto e su un campione. Nello specifico, una volta ripristinati sistemi e componenti critiche, viene: • avviata l'attivazione dei collegamenti di rete presso il sito alternativo; • testato l'accesso agli applicativi; • testato l'operatività giornaliera; **D2.2** Attivazione di parte dei servizi presso il sito di "Near BC" al fine di simulare l'operatività giornaliera, con riferimento ai processi definiti critici nelle BIA delle unità organizzative, e verifica del rispetto del RTO condiviso con i Clienti. Tale test viene effettuato da remoto e	Ufficio Sistemi / SINTEA / Unità organizzative	Annuale

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275

	su un campione. Nello specifico, una volta eseguita l'attivazione viene: • avviati i collegamenti di rete presso il sito di "Near BC"; • testato l'accesso agli applicativi; • testato l'operatività giornaliera;		
E. Indisponibilità della documentazione fondamentale (dati e documenti critici)	**E1.** Test di ripristino dei backup	Ufficio Sistemi	Annuale
F. Interruzione del funzionamento delle infrastrutture	**F1.** Test di continuità degli apparati afferenti l'infrastruttura (es. Gruppo Elettrogeno)	Ufficio Sistemi / RBRE	Annuale
G. Indisponibilità di dotazioni specifiche	Non sono previsti test essendo un'attività ordinaria eseguita dall'ufficio sistemi	N/A	N/A

Previnet® S.p.A. Società Unipersonale – Direzione e Coordinamento RBHOLD S.p.A.
Via E. Forlanini, 24 – 31022 Preganziol (TV) - Italia
tel +39 0422 174 5111– fax 0422 174 5025 – previnet@previnet.it – www.previnet.it
capitale sociale € 20.000.000 i.v. – Codice fiscale / partita IVA e n. iscrizione registro imprese Treviso 03567980275