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	**Area Pubblica in data 28 maggio 2021**
Soggetto a revisione	**Annuale**

INDICE

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

Public ☐
Confidential ☑
Restrict ☐

PREVINET S.p.A.

BUSINESS CONTINUITY PLAN

ESTRATTO

SOMMARIO

Versioni

#	Data	Autore	Principali modifiche
1	03/2011	Previnet	Prima emissione
2	04/2012	Previnet	Revisione annuale
3	11/2013	Previnet	Revisione annuale
4	10/2014	Previnet	Revisione annuale
5	11/2015	Previnet	Revisione annuale
6	12/2016	Previnet	Revisione annuale
7	10/2017	Previnet	Revisione annuale
8	10/2018	Previnet	Revisione annuale e adeguamenti
9	07/2019	Previnet	Revisione annuale e adeguamenti
10	05/2020	Previnet	Revisione annuale e adeguamenti

Legenda

Definizione	Descrizione
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.
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 impact analysis / Analisi di impatto del rischio	Documento che contiene l'analisi e valutazione dei rischi e delle minacce cui è soggetta ogni area di business di Previnet e relativi contromisure/controlli previsti
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)	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

1 Premessa e contesto di riferimento

Per rafforzare l'impegno a garantire adeguati livelli di continuità operativa, Previnet S.p.A. ha definito un piano di continuità operativa o business continuity plan (BCP) per la gestione di situazioni di crisi conseguenti a incidenti di portata settoriale, aziendale ovvero a catastrofi estese che colpiscano la società, uniformandosi in ciò alle normative vigenti a cui è soggetto il Cliente in qualità di operatore finanziario, e tenendo conto delle *best practices* definite a livello internazionale o nell'ambito degli organismi di categoria.

1.1 Certificazione ISO27001 e adempimenti in materia di sicurezza

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 ISO27001 compliant prevede l'attuazione di procedure e controlli, svolti dal personale aziendale, per il raggiungimento e mantenimento nel tempo degli obiettivi seguenti:

- Avere piena conoscenza delle informazioni gestite e consapevolezza della loro criticità;
- Garantire l'accesso sicuro alle informazioni;
- Garantire che le terze parti adottino procedure volte al rispetto di adeguati livelli di sicurezza, in relazione alla natura delle informazioni trattate;
- Gestire gli incidenti in modo proattivo, tempestivo ed efficace;
- Gestire la sicurezza fisica;
- Essere conformi ai requisiti di legge;
- Rispettare gli impegni di sicurezza stabiliti con le terze parti;
- Garantire la business continuity aziendale e il disaster recovery.

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).

2 Principi

2.1 Ambito del piano

Il piano di continuità operativa indica le conseguenze derivanti dall'interruzione del servizio causata da differenti scenari di crisi e definisce le misure di prevenzione e i presidi organizzativi e tecnici da attivare in caso di incidente.

La definizione del presente BCP e delle relative misure per il rientro dall'emergenza e per la salvaguardia degli archivi elettronici e funzionamento dei sistemi informativi è elaborata con approccio esteso, in conformità con la normativa di riferimento[1] e considerando **diversi scenari di crisi** (anche estesa e di blocco prolungato) basati sui **seguenti fattori di rischio**:

- distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche;
- indisponibilità di sistemi informativi critici;
- indisponibilità di personale essenziale per il funzionamento dei processi aziendali;
- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);
- alterazione o perdita di dati e documenti critici;
- danneggiamenti gravi da parte di dipendenti.

Parte integrante del Piano di continuità operativa è costituita dai documenti:

- **Risk Impact Analysis o RIA;**
- **Business Impact Analysis o BIA;**
- **Disaster Recovery Plan.**

2.2 Analisi di impatto: RIA e BIA

La definizione del piano di continuità operativa per Previnet è avvenuta in conseguenza allo svolgimento della preliminare **analisi di impatto** dove viene identificato il livello di rischio dei processi aziendali e vengono poste in evidenza le conseguenze dell'interruzione del servizio. L'analisi integra il presente piano ed è delineata nei seguenti documenti:

- **Risk Impact Analysis (o RIA)**: contiene l'analisi e valutazione dei rischi e delle minacce cui è soggetta ogni area di business di Previnet e relativi contromisure/controlli previsti;
- **Business Impact Analysis (o BIA):** individua il livello di rischio **dei processi aziendali** afferenti ogni area di business, identifica i processi critici per i quali deve essere garantito il funzionamento anche nel periodo di disastro e definisce il responsabile dei processi, le procedure informatiche di supporto, il personale addetto, le strutture logistiche interessate, le infrastrutture tecnologiche e di comunicazione utilizzate.

2.3 Disaster Recovery Plan

Il disaster recovery plan (o DRP) stabilisce 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 nel sito alternativo a quello di produzione.

[1] 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 "Continuità operativa" del Regolamento di attuazione degli articoli 4-undecies e 6, comma 1, lettere b) e c-bis) del TUF, Codice delle Assicurazioni Private (CAP, art. 30), Regolamento IVASS n. 38 del 2018 (art. 19, cc. 5 e 6), Articolo 258, paragrafo 3, degli Atti Delegati.

Per le sue applicazioni critiche e sistemiche, Previnet ha realizzato una soluzione di Disaster Recovery basata su una configurazione a due siti (primario e secondario 'cold site') con replica dei dati asincrona.
Il DR site o sito alternativo è rappresentato dalla sede di Sintea Servizi Informatici S.r.l., sita in via Perugia 56, Torino (situata a circa 400 km dal sito primario). Il sito alternativo può essere utilizzato, in caso di necessità, anche per periodi prolungati. Il sito di DR è già allestito e completo dei dispositivi e infrastrutture da utilizzare in caso di emergenza.

3 Ruoli e responsabilità

Ai fini della definizione del presente piano, nell'ambito della ripartizione di ruoli e responsabilità nella gestione della crisi, Previnet ha provveduto a:

- Definire ruoli e competenze degli organi aziendali e di tutte le risorse coinvolte dal BCP e DRP (vedi 3.1 e 3.2);
- Assicurare le risorse umane, tecnologiche e finanziarie adeguate per la gestione della crisi.

3.1 Comitato di Emergenza

Previnet ha istituito il Comitato d'emergenza le cui mansioni principali sono:

- Approvare il piano di continuità e le successive modifiche a seguito di adeguamenti tecnologici e organizzativi, accettando i rischi residui non gestiti;
- Approvare il piano delle verifiche periodiche dell'adeguatezza del BCP e relative misure di continuità operativa ed esaminare i risultati delle prove;

In caso di disastro, il comitato è responsabile di:

- Valutare lo stato di operatività dell'azienda al fine di individuare lo scenario realizzatosi;
- Eseguire la procedura di invocazione;
- Attivare il Gruppo Operativo di emergenza ai fini della collaborazione;
- Informare tempestivamente e nel continuo la Direzione (AD e CDA) e i responsabili delle varie aree aziendali (senior manager) circa la gestione ed evoluzione dell'evento di emergenza;
- Gestire (regolare inizialmente) le comunicazioni con i clienti;
- Individuare e gestire le risorse umane dedicate al servizio;
- Sovrintendere le operazioni di ripristino definite nel piano;
- Sovrintendere tutti i servizi aziendali durante il loro funzionamento nel sito dedicato al servizio;
- Sovrintendere le operazioni di ripristino del sito aziendale principale, attivando al momento opportuno la procedura di ripristino dei servizi in tale sito.

Il **Comitato** di Emergenza è composto dai seguenti referenti:

Nome	Area	Contatto
OMISSIS		

Per svolgere le proprie funzioni di valutazione dello scenario e esecuzione delle relative procedure, il **Comitato** può essere attivato da:

- Responsabile della sicurezza di Previnet;
- Dirigenti di ciascuna area di business di Previnet;
- in subordine, dai funzionari (quadri).

Le decisioni del Comitato sono verbalizzate da uno dei membri dello stesso e condivise / approvate immediatamente prima del termine della riunione.

3.2 Gruppo Operativo di Emergenza

Il Gruppo Operativo di Emergenza istituito da Previnet è composto da dipendenti di Previnet che hanno ricevuto **specifica formazione** circa le modalità di **gestione delle situazioni di emergenza**, con particolare attenzione alla prevenzione incendi, al primo soccorso ed alle misure di evacuazione dei lavoratori, nella fattispecie è composto dai seguenti referenti:

Funzione	Rappresentante (nome)
Rappresentante dei lavoratori per la sicurezza (RLS)	• [OMISSIS] • [OMISSIS] • [OMISSIS]
Addetti antincendio	• [OMISSIS] • [OMISSIS] • [OMISSIS] • [OMISSIS] • [OMISSIS] • [OMISSIS]
Addetti al primo soccorso	• [OMISSIS] • [OMISSIS] • [OMISSIS] • [OMISSIS]
Referenti operativi per ciascuna area di business aziendale	Come da BIA per l'area di business e servizio di riferimento. In caso di assenza o indisponibilità il comitato di emergenza provvederà a nominare il sostituto.

Il Comitato di emergenza ed il Gruppo operativo si riuniscono solo in caso di emergenza (cioè se attivati, nelle modalità indicate sopra) o, in forma ridotta, per coordinare le sessioni annuali di test (vedi § 6 Verifiche e controlli delle misure di continuità operativa).

4 Presupposti per la gestione delle misure di continuità

4.1 Integrità dei dati e procedure di back up

Previnet provvede ad effettuare una volta al giorno il salvataggio su disco di un immagine consistente **dei database** e più volte al giorno il salvataggio su disco delle transazioni, per poter ricostruire un database in un qualsiasi istante precedente ad un'eventuale corruzione. Le operazioni di salvataggio vengono eseguite in linea e non comportano un degrado delle prestazioni del sistema.

I server di Previnet sono virtuali e risiedono su un cluster hardware ridondato in tutte le sue componenti e dimensionato per sopportare eventuali danni fisici, in questo modo eventi più comuni come ad esempio il danneggiamento di un disco ma anche più gravi come il danneggiamento di un server fisico non danno luogo ad alcuna perdita.

I server virtuali più critici vengono costantemente replicati nell'infrastruttura di Disaster Recovery, in questo modo i tempi di ripristino sono ridotti drasticamente.

Inoltre **tutti i server** e quindi tutti i dati di produzione vengono sottoposti a procedura di backup che salva un immagine quotidiana, preservata per almeno una settimana, ed un immagine mensile, preservata per dieci anni. Le immagini sono salvate su un sistema disco dedicato e replicate quotidianamente in analogo sistema situato nel sito di Disaster Recovery. Per conservazione storica le immagini mensili sono anche duplicate su cassetta.

Le procedure di backup e custodia di cassette e copie di sicurezza sono eseguite con regolarità nel rispetto delle procedure ISO27001.

Tutti i dati importanti (documenti, fogli di calcolo, database eventuali di supporto) risiedono esclusivamente su dischi di rete, gestiti secondo una procedura predefinita di backup, e non all'interno dei singoli PC degli utenti.

Si dichiara infine che tutti i dati gestiti da Previnet risiedono in Italia.

4.2 Copertura e caratteristiche del piano

Oltre a quanto specificato nel DRP, si dichiara quanto segue:

- Non sarà ripristinato il contenuto dei PC personali: ogni utente, presso il sito di Recovery, disporrà di un PC dotato degli strumenti di produttività individuale (Office, posta elettronica) ma del tutto vergine nel contenuto;
- I dati gestionali disponibili saranno aggiornati in base al RPO (*Recovery Point Objective)* dichiarato nel paragrafo 4.4. Il meccanismo di ripristino prevede infatti che i sistemi vengano riallineati utilizzando i salvataggi su nastro o disco che saranno disponibili presso Previnet o il sito di Disaster Recovery;
- Sulla base degli interfacciamenti di sistema previsti dal modello operativo adottato per svolgere i servizi indicati nel Contratto di servizio tra Previnet e il Cliente, le soluzioni di contingenza e le modalità di scambio di informazioni e comunicazioni verrà indicata nel documento di BIA;
- Le attività di sviluppo software saranno bloccate nel periodo di disastro;
- Le risorse dotate di PC portatile potranno intervenire in caso di anomalie operando da casa propria (autenticazione con nome utente e password) o recandosi momentaneamente presso il sito di Recovery;
- La tempistica con la quale devono essere ripristinati i processi operativi viene stimata dai singoli Referenti di settore ed è costituita dai tempi di analisi degli eventi, identificazione dello scenario di riferimento e decisione delle azioni da intraprendere (Comitato di Emergenza e Gruppo operativo di emergenza) e dalla ripartenza del processo attraverso l'attuazione degli interventi tecnici e organizzativi previsti. Nello specifico, per quanto concerne i servizi dell'area, si rimanda ai documenti di BIA e RIA specifici per ogni business unit;
- Sono stati inclusi nell'analisi tutti i processi di business identificando quelli per i quali deve essere garantito il funzionamento anche nel periodi di crisi. È stata prevista

l'operatività di tutti i processi di business seppure con una minore efficienza legata all'utilizzo di un numero ridotto di risorse umane e il ricorso a procedure di "contingency" diverse da quelle ordinarie.

4.3 Comunicazioni e notifiche relative all' attivazione/ripristino BCP con il Cliente

Tutte le comunicazioni verso clienti, fornitori e istituzioni sono regolate dal comitato di emergenza (di concerto con il gruppo operativo di emergenza) che tempestivamente individua una figura alla quale affida l'incarico di portavoce con il mandato di veicolare attraverso i responsabili delle varie aree aziendali (senior manager) le notizie riguardanti la gestione ed evoluzione dell'evento di emergenza.

Le comunicazioni verso i Clienti saranno gestite dai referenti di progetto. Per quanto attiene alla comunicazione verso il Cliente, Previnet si impegna e comunicare le cause del problema e la stima della durata dell'interruzioni dei servizi interessati, con la massima diligenza possibile.

E' fatto divieto a chiunque non autorizzato a divulgare informazioni non autorizzate e non approvate dal Comitato di emergenza.

4.4 Tempi di Ripristino in caso di DR

Con la sigla **RTO** (*Recovery Time Objective*), si intende il periodo di tempo che intercorre dalla dichiarazione dello stato di crisi e l'istante in cui il processo è ripristinato ad un livello di servizio predefinito. L'RTO è costituito dai tempi di:

- Analisi degli eventi, individuazione dello scenario e decisione delle azioni da intraprendere (vedi § 5 Scenari e procedure operative per la gestione delle emergenze);
- 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. Le procedure sono in grado di ripristinare i sistemi con dati non più vecchi di 24 ore dall'evento disastroso.

Con la sigla **RPO** (*Recovery point objective*) si intende l'istante di salvataggio dei dati fino al quale è garantita l'integrità degli stessi nei siti primari e alternativi.

In sintesi vale la seguente tabella:

RTO	72 ore
RPO	24 ore

5 Scenari e procedure operative per la gestione delle emergenze

Il Comitato di Emergenza ed il Gruppo Operativo di emergenza di Previnet hanno individuato i seguenti scenari di crisi, basati sui fattori di rischio conseguenti a eventi naturali o attività umana, inclusi danneggiamenti gravi da parte di dipendenti.

Le procedure di continuità operativa definite di seguito, in modo chiaro e dettagliato, possono essere eseguite anche da risorse non impegnate nell'ordinaria attività nei processi cui si riferiscono. Il personale coinvolto viene addestrato sulle misure di Business Continuity e partecipa alle sessioni di verifica delle misure di continuità operativa.

Le risorse umane individuate per garantire il funzionamento dei processi potranno essere solo una frazione di quelle normalmente disponibili.

5.1 Scenario (A) – Distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche

5.1.1 Descrizione

Nello scenario A, la situazione è talmente critica da rendere inutilizzabili il piano terra ed il primo piano della sede e le apparecchiature critiche ivi collocate.

5.1.2 Misure operative

Se si realizza lo scenario A, si dovrà attivare il servizio di DR per i sistemi, presso il sito alternativo di Sintea.

1) Come **attività preliminari** il comitato di emergenza (**o delegato**) dovrà:
   - **Informare la Direzione** (AD – CdA) dello stato di crisi e **telefonare ai referenti di progetto / clienti / controparti / fornitori** per la dichiarazione di disastro (per i riferimenti, vedasi Appendice A al presente documento);
   - Attivare la procedura di Invocation, come da Manuale di invocazione del servizio contrattualizzato con il fornitore di servizi di DR;
   - **Definire il piano di spostamento delle risorse dalla sede disastrata** - o altro luogo di partenza - **al sito alternativo** per svolgere le attività di attivazione del DR, definendo dei gruppi di lavoro in base alla priorità. Verosimilmente il primo gruppo che dovrà spostarsi presso il DR site sarà costituito da:
     - [OMISSIS]
     - [OMISSIS]
   - Organizzare il trasferimento delle risorse (sulla base delle priorità di trasferimento decise al punto sopra), avendo valutato la migliore opzione, dalla sede disastrata – o altro luogo di partenza – al sito alternativo **attivandosi in primo luogo per il reperimento/prenotazione del mezzo di trasporto e in secondo luogo per il vitto e alloggio**.

     Alcune **opzioni di trasferimento** potrebbero essere:

     [OMISSIS]

     Per i servizi di trasporto localizzati nelle vicinanze della sede disastrata, si riportano i seguenti contatti:

     [OMISSIS]

     Per la prenotazione di posti treno si consigliano:

     [OMISSIS]

     Per le possibili strutture da contattare:

     [OMISSIS]

2) Mentre avviene lo spostamento delle risorse da Preganziol alla sede alternativa di Torino, i colleghi di Sintea S.r.l. operano al ripristino dei sistemi e all'allestimento delle PDL, come indicato nel piano di DR tra Previnet e Sintea;
3) L'attivazione del servizio di recupero e **ricostruzione dei sistemi** nel sito alternativo DR avviene nelle modalità definite nel piano di Disaster Recovery di Previnet;
4) Per tutto il periodo del disastro, l'attività per il ripristino della sede danneggiata verrà seguita dalla Direzione - AD e CDA - e dai suoi collaboratori (ad esempio Senior Manager) per la parte strutturale e la parte informatica. Vale il seguente processo di informativo/decisionale:
    - il **Comitato di Emergenza informa la Direzione** circa l'evoluzione dell'evento di emergenza;
    - La **Direzione** (e collaboratori) **relaziona giornalmente** su quanto deliberato **il Comitato di Emergenza il quale di conseguenza provvede** a tenere **costantemente informati** circa la gestione ed evoluzione dell'evento di emergenza, le soluzioni e misure da intraprendere per il ritorno alla sede principale e alla normale operatività lavorativa:
        - **i componenti del gruppo operativo di emergenza**
        - **i responsabili delle varie aree aziendali** comprese le **funzioni trasversali** come Sistemi e Infrastrutture e Logistica
    - In seguito, **i responsabili delle aree aziendali** (e collaboratori) **e i responsabili delle funzioni trasversali organizzano le attività delle risorse gestionali/operative/tecniche coinvolte,** con la miglior diligenza, informandole dei task assegnati e delle modalità/tempi di esecuzione;
    - I responsabili delle aree aziendali (e collaboratori) si occupano della comunicazione verso i Clienti/fornitori.
5) Per un eventuale **recupero dei materiali** rimasti presso la sede disastrata le persone interessate debbono contattare il Responsabile della sicurezza (RLS) di Previnet. L'RLS si coordinerà col responsabile dei Vigili del Fuoco per poter recuperare il materiale ritenuto indispensabile. Ciascun utente dovrà predisporre un elenco con la descrizione del materiale che desidera recuperare (indicandone importanza e scopo) e della relativa collocazione (piano, stanza, armadio, etc.) per facilitarne il reperimento. Tale elenco dovrà esser trasmesso al comitato di emergenza e conservato privatamente dall'utente Previnet dove ritiene più opportuno;
6) Nel caso di permanenza presso siti alternativi per un periodo prolungato di tempo ovvero per la gestione di processi critici, la Direzione valuterà la migliore soluzione alternativa, ad esempio:
    - Telelavoro / Smart working;
    - Affitto di spazi di lavoro dotati di connessione internet (esempio OMISSIS).
7) Una volta ricevuta dalla Direzione la disposizione per il ritorno **alla sede ristrutturata o allestita una sede alternativa**, **il comitato di emergenza pianificherà** lo svolgimento delle **procedure inverse** di quanto indicato nei piani d'azione per il DR. Inizieranno i test sul patrimonio informatico e tecnologico, e dopo aver costatato che tutte le schede comprendenti le certificazioni degli applicativi sono resi disponibili per gli utenti, si procederà al rientro in Sede del personale dislocato presso il sito di DR e successivamente di tutto il personale societario;
8) Le **notifiche per il ritorno alla normalità** saranno trasmesse secondo lo schema di notifica seguito per la comunicazione del disastro indicato al punto 1), ove in questo caso si provvederà a comunicare la cessazione della condizione.

5.2 Scenario (B) – Parziale distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche

5.2.1 Descrizione

Nello scenario B, la situazione è tale per cui per esempio è inutilizzabile il piano terra e le apparecchiature critiche ivi collocate mentre è utilizzabile il primo piano della sede (o viceversa), il comitato di emergenza dovrà valutare se spostare le risorse con le macchine negli uffici e sale riunioni che si trovano nel corpo centrale dell'edificio, o se usufruire della disponibilità di PDL da altre aree aziendali.

5.2.2 Misure operative

1) Il comitato di emergenza valuta la gravità della situazione e decide se:
    a. portare le risorse e le PDL nelle sale riunioni;
    b. utilizzare le PDL di altre aree aziendali;
2) Il comitato di emergenza informa la Direzione e convoca i responsabili dei vari uffici (come da BIA per area di business e servizio di riferimento) per informare tutti dell'accaduto e della strategia adottata:
    a. Nel caso a. si provvederà a collocare le PDL nelle sali riunioni dello stabile e a far accomodare le risorse;
    b. Nel caso b. il comitato di emergenza attiva l'ufficio sistemisti dell'area IT per adeguare le PDL prescelte ai servizi dell'area aziendale danneggiata;
3) L'attività per il **ripristino del piano danneggiato** verrà seguita dalla Direzione - AD e CDA - e dai suoi collaboratori (ad esempio Senior Manager) per la parte strutturale e la parte informatica;
4) Per un eventuale **recupero dei materiali** rimasti presso il piano disastrato, vale quanto già espresso nel paragrafo precedente (vedi §5.1.2);
5) Una volta ricevuta la disposizione per il ritorno **al piano ristrutturato**, il comitato di emergenza pianificherà lo svolgimento delle procedure inverse di quanto indicato al punto 2, a seconda che si verifichi il caso a o b.

5.3 Scenario (C) – Indisponibilità di sistemi informativi critici

5.3.1 Descrizione

Se il danneggiamento riguarda solo le componenti informatiche e/o telematiche, **in funzione delle condizioni e della gravità, si può dichiarare il disastro** (scenario A, §5.1) **oppure provvedere alla sostituzione** delle apparecchiature danneggiate e più in generale al ripristino delle PDL.

Nel caso di malfunzionamenti non gravi o che non hanno significativi impatti sull'operatività corrente e sul servizio da erogare al Cliente, la continuità operativa e del business è garantita dalla normale gestione della manutenzione correttiva.

5.3.2 Misure operative

Si premette che il sistema Elaborazione dati adottato da Previnet - ad oggi il più diffuso nei centri di elaborazione dati e noto con il nome di "cluster applicativo di elaboratori" - tollera il fermo contemporaneo di più di un elaboratore, senza impatti nell'erogazione del servizio. Ciascun elaboratore costituente il cluster è a propria volta duplicato nelle componenti fondamentali e quindi in grado di resistere al guasto di un componente senza dover trasferire ad altro sistema le risorse gestite. Un sistema del cluster costituisce l'unità di stand-by deputata a farsi carico delle risorse gestite da uno degli altri sistemi in caso di necessità. Ciò posto, le misure da adottare sono le seguenti:

1) **Il comitato di emergenza attiva** il gruppo **operativo di emergenza** per il ripristino delle PDL nel più breve tempo possibile. Tutte le manutenzioni sono svolte da personale interno di Previnet;
2) Nel frattempo le PDL saranno temporaneamente sostituite da PDL di backup o postazioni portatili. In funzione della tipologia di evento che ha causato il malfunzionamento di tipo scenario C, potranno o meno essere disponibili alcune risorse (ad esempio informatiche) / funzioni / applicazioni informatiche;
3) Nel caso in cui tale indisponibilità dovesse impedire l'erogazione del servizio, ancorché nella sua forma minima, il comitato di emergenza dovrà valutare se attivare parzialmente lo scenario (A) (vedasi paragrafi precedenti) limitatamente a determinate risorse "Chiave" che potranno quindi operare con PDL verosimilmente funzionanti dalla sede di Torino oppure da postazioni portatili. Le altre risorse proseguiranno il servizio dalla Sede Principale utilizzando le componenti non danneggiate;
4) La procedura proseguirà fino al totale e completo ripristino della situazione ante crisi;
5) In merito alle **notifiche per il ritorno alla normalità** vale, nel caso di attivazione parziale dello scenario (A), lo stesso schema di notifica indicato per la comunicazione del disastro, ove in questo caso si provvederà a comunicare la cessazione della condizione. Nel caso in cui lo scenario (C) non preveda la parziale attivazione dello scenario (A), la comunicazione di notifica per il ritorno alla normalità **riguarderà comunicazione interna Previnet**.

5.4 Scenario (D) – Indisponibilità di personale essenziale per il funzionamento dei processi aziendali

5.4.1 Descrizione

Se **più del 50% (soglia di attivazione) del personale operativo/gestionale e informatico** di riferimento per l'area aziendale **non è disponibile**, il Comitato di emergenza, in base alla gravità della situazione, decide se avvalersi delle risorse presenti nelle altre unità operative.

5.4.2 Misure operative

1) Il comitato di emergenza attiva il gruppo operativo di emergenza per lo spostamento di alcune risorse da altri uffici o altre aree aziendali per garantire l'operatività concordata e gli SLA condivisi con il cliente;
2) Sono identificate ed eventualmente addestrate le risorse chiave di Previnet che saranno coinvolte nelle attività descritte nel DRP;
3) C'è un sostituto per ciascuna delle risorse chiave, che interverrà nella gestione delle attività descritte nel DRP in mancanza della risorsa titolare. In linea generale, il sostituto verrà individuato tra le figure professionali che, nella gerarchia dell'organigramma Aziendale, si trova allo stesso livello o al livello immediatamente inferiore rispetto a quello occupato dalla risorsa chiave

I casi di indisponibilità di personale che **non determinano il superamento** della **soglia di attivazione** saranno gestiti secondo le normali procedure di ridondanza e backup risorse - definite per ciascuna gestione / Cliente, dai dirigenti di area, in subordine dai quadri dell'area interessata, in subordine dai referenti di ciascun Ufficio / gestione / Cliente. Sotto la soglia di attivazione, lo scenario non si considera di reale emergenza.

Il piano di continuità aziendale, per i processi afferenti all'area -, non prevede personale addestrato in un sito secondario.

5.5 Scenario (E) – Indisponibilità sub–fornitore

5.5.1 Descrizione

Lo scenario (E) si realizza in caso di **indisponibilità dei sub-fornitori** per attività accessorie di:

- **Postalizzazione;**
- **Data entry;**
- **Gestione documentale (Digitalizzazione, fase istruttoria, archiviazione sostitutiva);**
- **Outbound call.**

5.5.2 Misure operative

Si premette che non si ritiene che lo scenario (E) possa verosimilmente costituire grave crisi considerato che nessuna attività *core* per il Cliente è demandata a personale esterno a Previnet e considerato il fatto che Previnet è strutturata per poter gestire internamente le attività accessorie sopra descritte, con tempi di reazione sufficienti a garantire la continuità operativa. Ciò posto, le misure adottate sono:

1) Il comitato di emergenza analizza e valuta la gravità dello scenario realizzatosi e contatta il gruppo operativo di emergenza per l'attivazione del subfornitore di backup o la temporanea internalizzazione delle attività fino alla chiusura dello scenario (E);
2) Il comitato di emergenza informa i referenti delle aree di business / processo, i quali provvederanno ad organizzare le attività operative delle risorse gestionali coinvolte.

Qualora le condizioni palesemente non richiedano l'attivazione del comitato di emergenza e del gruppo operativo di emergenza, quindi lo scenario non è di reale emergenza ma di semplice attenzione, i Referenti delle aree di business hanno il compito di gestire la situazione e l'operatività nel rispetto di quanto stabilito contrattualmente ed eventualmente concordato operativamente con ciascun Cliente.

5.6 Scenario (F) – Interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazioni, reti interbancarie, mercati finanziari)

5.6.1 Descrizione

Lo scenario F si realizza in caso di interruzione del funzionamento di una o più infrastrutture necessarie all'erogazione dei servizi di Previnet.

5.6.2 Misure operative

Previnet S.p.A. ha costruito il proprio Sistema Informativo in un'ottica di High Availability e Fault Tollerance. Di seguito vengono descritte le misure previste, con riferimento ai diversi ambiti:

- Dal punto di vista **dell'alimentazione elettrica**, tutte le macchine sono alimentate tramite **gruppi di continuità (UPS).** Tali dispositivi sono conformi alle norme EN50091-1/IEC62040-1 (Safety), IEC62040-2 (Emissions), IEC62040-3 (Performance and test) e permette una manutenzione in linea di batterie e circuiti. In caso di mancanza di alimentazione elettrica i gruppi di continuità intervengono mantenendo in funzione le apparecchiature fino all'accensione (automatica) dei gruppi elettrogeni di supporto. Tali gruppi sono in grado di generare corrente elettrica a fronte di una mancanza di tensione di rete potenzialmente per un tempo indeterminato. Il dispositivo garantisce tempi di intervento inferiori al minuto. Previnet ha inoltre previsto **sistemi complementari per il controllo ambientale** (esempio impianto di condizionamento) ridondati al fine di garantire continuità a fronte di un guasto;
- **Reti di telecomunicazioni:** La gestione della sicurezza della parte di connettività è in carico alle procedure definite nel ISMS di Previnet. Per i servizi Internet, Previnet si avvale di **due**

differenti provider (ISP) che la connettono ai *backbone* nazionali in fibra ottica. Con uno dei due provider è stato attivato un ulteriore collegamento di backup automatico in ponte radio;

- **Reti interbancarie:** i casi di indisponibilità delle reti interbancarie sono disciplinati nei piani di contingenza con tra Previnet e Fornitori / Clienti;
- **Mercati finanziari:** i casi di indisponibilità dei mercati finanziari sono disciplinati nei piani di contingenza con tra Previnet e Fornitori / Clienti.

5.7 Scenario (G) – alterazione o perdita di dati e documenti critici

5.7.1 Descrizione

Lo scenario G include tutti gli eventi di effetto alterativo o distruttivo su dati e documenti critici, conseguenti a eventi naturali o attività umana inclusi danneggiamenti gravi da parte di dipendenti.

5.7.2 Misure operative

Si premette che, per limitare la perdita dei dati o l'alterazione degli stessi Previnet ha previsto le seguenti misure:

- **Previnet impiega tecnologie di interscambio dati** (connessioni di rete, rete locale e connessioni geografiche verso i diversi interlocutori aziendali e verso Internet) **diverse per ciascun tipo di collegamento** e garantisce che non vi siano fermi delle attività gestionali sia attraverso la **ridondanza nei percorsi di rete per i collegamenti principali** sia attraverso **procedure di contingency per i rimanenti collegamenti** – queste ultime assicurano comunque il completamento delle attività gestionali nei tempi previsti;
- I dati in transito da/verso servizi Internet sono **crittografati** mediante protocolli sicuri (TLS / HTTPS). Per gli scambi via internet vengono implementati flussi cifrati (GPG) o protetti da una soluzione di cloud privata (WebTransfer) ospitata nei data center aziendali, sviluppata internamente secondo i principi espressi nel nuovo regolamento europeo sulla protezione dei dati (GDPR);
- Per **l'archiviazione dati** (scritture dei dati su disco) **Previnet** utilizza un sistema di **Storage Area Network (SAN) e un Disk Array** di livello ***enterprise*** il quale garantisce l'assenza di interruzioni dei sistemi connessi e la protezione dei dati (dal rischio di perdita/corruzione) anche in caso di completo danneggiamento della metà dei suoi componenti;
- Previnet utilizza una soluzione di backup di livello enterprise con la quale provvede a salvare con frequenza quotidiana tutti i dati trattati. Copie dei backup sono riportati quotidianamente nel sito di DR;
- Per la protezione da software dannosi, virus e malware, intrusioni dall'esterno, Previnet è dotata di sistema antispam, antivirus di ultima generazione nei client e nei server, firewall centralizzati in configurazione a doppio bastione;
- Previnet ha definito un codice etico e di condotta e linee guida, sensibilizzando i propri operatori, con appositi ordini di servizio, oltre che con la diffusione del proprio codice disciplinare interno, a custodire e non diffondere informazioni riservate, le proprie credenziali di accesso sia ai computer che agli applicativi utilizzati, a non lasciare incustodita la propria postazione di lavoro (se prima non ha provveduto alla disconnessione della propria utenza);
- Sono state definite **misure specifiche per gli sviluppi e gli aggiornamenti software** nel rispetto dei principi di privacy by design e by default richiesti dal GDPR;
- Previnet ha definito il processo di data breach o notifica di violazione dei dati personali all'autorità di controllo e all'interessato (ai sensi degli artt. 33 e 34 del GDPR);
- Si ricorda infine che, sulla base del Registro dei trattamenti e della valutazione di rischio privacy Previnet ha aggiornato le sue misure di sicurezza (fisica e logica), tecniche ed organizzative, nel rispetto dell'art. 32 del GDPR. Le misure e i controlli adottati comprendono quelli della norma ISO27001, standard internazionale per la sicurezza delle informazioni,

riconosciuta quale base per la norma internazionale sulla protezione dei dati personali (ISO 29100).

Ciò posto, al verificarsi dello scenario G, sono previste le seguenti misure operative:

1) A fronte della segnalazione, il comitato di emergenza (anche in forma ridotta ovvero composto dai dirigenti area) si riunisce per valutare la gravità della situazione e, se necessario, attiva ulteriori procedure (e.g. Procedura di Gestione del Data_Breach, Procedura di segnalazione degli incidenti privacy, procedura sanzionatoria);
2) In base alla gravità dello scenario, il comitato di emergenza valuta l'eventuale comunicazione verso la Direzione, Clienti/Fornitori coinvolti;
3) Il comitato di emergenza presidia l'evoluzione dello scenario.

5.8 Scenario (H) – Situazioni di crisi gravi anche non connesse ad eventi comportanti distruzioni materiali

5.8.1 Descrizione

Lo scenario H include tutti gli eventi che determinano gravi crisi a livello locale o globale, conseguenti a eventi naturali o attività umana anche non connessi ad eventi comportanti distruzioni materiali. Rientrano in questo scenario ad esempio attacchi biologici, chimici, nucleari, atti terroristici/bioterrorismo, incidenti ambientali, blocco totale o parziale dei sistemi di trasporto, pandemie, epidemie/malattie.

5.8.2 Misure operative

Si premette che, considerata la tipologia di attività professionali svolte, Previnet S.p.A. assicura a tutti i dipendenti la predisposizione al tele-lavoro tramite:

- Completo accesso alla postazione di lavoro anche a distanza o da remoto, anche fornendo ai dipendenti che non ne disponessero, la necessaria dotazione hardware (PC portatile, collegamento Internet, accesso/abilitazione da remoto). A tal fine, ogni area mantiene una mappatura aggiornata circa le disponibilità di dotazioni personali di ogni risorsa;
- Collegamento telefonico (chiamate interne / esterne) anche a distanza o da remoto.

Il **piano di contingenza da definirsi** in caso di attuazione dello scenario H deve considerare i seguenti punti:

- **LAVORO DA REMOTO**: definire modalità e lavoratori coinvolti, considerando eventuali casi a rischio (ad esempio lavoratori che soffrono di patologie a rischio attestate dal SSN, previa presentazione dell'attestazione del medico curante in cui si dichiara la necessità di applicare le condizioni agevolate di lavoro da remoto ovvero a rischio in ragione della zona di provenienza intesa come domicilio/residenza);
- **MEETING E TRASFERTE:** definire eventuali riduzioni/annullamenti di riunioni interne / con ospiti esterni e/o trasferte, prediligendo le videoconferenze, gli scambi via mail o telefonici;
- **MODALITA' DI COMUNICAZIONE / CONTATTO** con i colleghi anche utilizzando, ai fini di una efficiente gestione dell'emergenza, i contatti personali (cellulare ed e-mail). A tal fine, è di competenza dell'ufficio amministrazione del personale mantenere aggiornate le informazioni a propria disposizione su domicilio/residenza e i contatti privati di ogni dipendente**;**
- **FORNITORI:** definire regolamentazione accessi alla sede da parte di fornitori;
- **MENSA:** definire eventuali presidi igienico-sanitari aggiuntivi, estensione oraria del servizio offerto e conseguente estensione della fascia di flessibilità per la pausa pranzo e nuova turnazione, eventuale riduzione del menu, eventuale totale o parziale sospensione del servizio;

- **PREVENZIONE**: definire, attuare e promuovere l'adozione di misure di prevenzione personali e/o da attuarsi nell'ambiente di lavoro anche sulla base di eventuali comunicazioni ricevute dal Sistema Sanitario Nazionale e/o Ministero della Salute o altro (esempio sanificazione degli ambienti).

Ciò posto, al verificarsi dello scenario H, sono previste le seguenti misure operative:

1) Il Comitato di Emergenza informa la Direzione circa l'evoluzione dell'evento di emergenza;
2) Il comitato di emergenza (anche in forma ridotta ovvero composto dai dirigenti area) convoca i responsabili dei vari uffici (come da BIA per area di business e servizio di riferimento) per valutare la gravità della situazione e di conseguenza definisce un piano di contingenza per l'applicazione delle misure identificate. Con riferimento all'attivazione del lavoro a distanza, il piano stabilisce le percentuali di attivazione di tale misure per le singole aree operative definite sulla base della gravità dello scenario. Il piano viene presentato alla Direzione per approvazione e per raccogliere eventuali richieste di variazione;
3) Il comitato di emergenza condivide con la Direzione la strategia operativa identificata per validazione o per raccogliere eventuali indicazioni specifiche e successivamente informa i responsabili delle varie aree aziendali comprese le funzioni trasversali come Sistemi e Infrastrutture e Logistica circa l'avvio del piano di contingenza così come approvato dalla Direzione, dando attuazione alle attività delle risorse gestionali/operative/tecniche coinvolte come definito dal piano di contingenza, con la miglior diligenza, informandole dei task assegnati e delle modalità/tempi di esecuzione;
4) I responsabili delle aree aziendali (e collaboratori) si occupano della eventuale comunicazione verso i Clienti/fornitori come anche del monitoraggio nel continuo del rispetto dei livelli di servizio;
5) Il comitato di emergenza relaziona giornalmente la Direzione (anche tramite verbali scritti) circa la gestione ed evoluzione dell'evento di emergenza, le soluzioni e le misure intraprese come anche il rispetto dei livelli di servizio;
6) Eventuali variazioni al piano ritenute opportune dal comitato di emergenza, sulla base delle evidenze raccolte anche dai responsabili delle aree aziendali (e collaboratori) sono presentate alla Direzione che valida o integra le proposte del comitato di emergenza e sempre verbalizzate;
7) In funzione dell'evoluzione dello scenario e di eventuali disposizioni normative, la Direzione e il comitato di emergenza stabiliscono tempistiche e modalità di ritorno in sede (ad esempio mediante turnazione o alternanza) e le comunicano a tutti i dipendenti. Ogni decisione viene verbalizzata.

6 Verifiche e controlli delle misure di continuità operativa

L'analisi di impatto ed i conseguenti piani per la continuità operativa sono rivisti annualmente e aggiornati sulla base di quanto appreso dalle verifiche effettuate, dall'individuazione di nuovi rischi e minacce, nonché dai cambiamenti degli obiettivi e dalle priorità di ripristino, nonché da eventuali rilievi durante le fasi di certificazione esterna.

Le modalità di verifica delle misure di continuità operativa dipendono dalla criticità dei processi e rischi ravvisati e dallo scenario di riferimento. Con frequenza almeno annuale:

- Il responsabile del piano (e del Contratto) per la business unit/servizio di competenza definisce (o rivede/integra) l'elenco dei test da eseguire per ciascuno scenario, sulla base delle esigenze correnti e dei mutati scenari organizzativi, operativi ed infrastrutturali nonché pianifica l' esecuzione delle verifiche, di concerto con il Comitato di Emergenza (anche in forma ridotta);
- Il comitato di emergenza (anche in forma ridotta) ed eventualmente il gruppo operativo di emergenza si riuniscono e coordinano l'esecuzione dei test relativi agli scenari sopra descritti

al fine di mettere in atto le soluzioni previste dal piano di emergenza. Per i processi critici le verifiche prevedono il coinvolgimento degli utenti finali e delle controparti rilevanti;

- I risultati delle verifiche vengono documentati, archiviati e inviati alle unità operative coinvolte (responsabili delle aree di business) e al Comitato di Emergenza. Eventuali punti di miglioramento/inefficienze messe in luce dal test vengono analizzate e, ove necessario, riportate a modifica del piano di emergenza del presente documento.

6.1 Modalità di verifica delle procedure di BC e DR

Le modalità di verifica sono differenti a seconda degli scenari e prevedono comunque l'attivazione dei collegamenti di rete presso il sito alternativo e l'esecuzione delle procedure batch con controllo della funzionalità e delle prestazioni del sito alternativo.

I test sono eseguiti dal personale normalmente incaricato a svolgere i servizi e relative attività e vengono utilizzati preferibilmente dati di produzione. Circa le modalità operative di verifica degli scenari:

- **Lo scenario (A)** viene annualmente testato simulando OMISSIS
- **Lo scenario (B)** viene annualmente testato simulando OMISSIS;
- **Per lo scenario (C)** annualmente viene simulata OMISSIS;
- **Per lo scenario (D)** annualmente viene simulata OMISSIS;
- **Per lo scenario (E)** annualmente viene simulata OMISSIS;
- **Per lo scenario (F)** annualmente viene simulato OMISSIS;
- **Per lo scenario (G)** annualmente viene svolto OMISSIS;
- **Per lo scenario (H)** annualmente viene verificato OMISSIS.

7 Conclusioni

[OMISSIS]

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.

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.

I responsabili del sistema informatico sono:

- 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).