BCP Piano di gestione della Continuità Operativa e Piani di Recovery

PCO/BCP

Versione: Estratto Pubblico di DMP017PP

Autorizzazione n°2 del 31/07/2023

ATTENZIONE IN CASO DI:

- **Livello 4 -** CRISI – utilizzare il capitolo 11
- **Livello 3 -** EMERGENZA – utilizzare il capitolo 10
- **Livello 2 -** INCIDENTE – utilizzare il capitolo 9
- Livello 1 – NORMALE – proseguire nella lettura

INDICE

1 DEFINIZIONI ACRONIMI E TERMINI

Acronimo/Termine	Definizione
BIA	Business Impact Analysis o Analisi di Impatto
CO	Continuità Operativa
CCO	Comitato Continuità Operativa
KPI	Key Performance Indicator
PCO/BCP	Piano di Continuità Operativa
RCO	Responsabile del piano di Continuità Operativa
RP	Responsabile di Processo
SGCO	Sistema di Gestione della Continuità Operativa
SPOF	Single Point of Failure
Stakeholder	Portatori d'interesse
RTO	Recovery Time Objective - Tempo per tornare operativi, ovvero tempo che intercorre tra il disastro e il completo ripristino dei sistemi
RPO	Recovery Point Objective - Metrica che indica il tempo trascorso dall'ultima replica dei dati all'evento dannoso
MBCO	Minimum Business Continuity Objective

2 INTRODUZIONE

Il presente documento descrive il piano per la continuità operativa, contiene tutti gli elementi utili a comprendere le metodologie utilizzate e le scelte effettuate per garantire di poter far fronte ad eventi avversi.

In condizioni di operatività normale si presuppone venga letto tutto in modo da avere un quadro completo ed esaustivo dell'argomento mentre in condizioni di utilizzo durante un evento avverso l'utilizzatore viene indirizzato nel punto esatto dove sono presenti le istruzioni da seguire.

Come indicato in copertina e ribadito nel testo sono stati previsti 4 livelli di operatività, i livelli sono anche differenziati per colore per facilitare l'utilizzo in condizioni di stress:

- Livello 1 – verde NORMALE
- Livello 2 – giallo INCIDENTE
- Livello 3 – arancio EMERGENZA
- Livello 4 – rosso CRISI

La Gestione della Continuità Operativa è un processo strategico e tattico che permette ad un'organizzazione di avere una risposta a qualunque avvenimento e interruzione del Business che può avere impatto sui processi aziendali che contribuiscono al "core business" dell'azienda, garantendo un livello di servizio minimo accettabile predefinito.

La "Gestione della Continuità Operativa" si pone l'obiettivo di individuare e dettagliare le attività che l'Organizzazione deve attuare al fine di implementare un processo di Continuità Operativa che permetta la sopravvivenza dell'azienda e garantisca la capacità di reagire agli incidenti, rispondere alle emergenze e alle calamità. Deve essere adeguatamente e puntualmente gestito, periodicamente rivisto, testato ed eventualmente adattato ai mutamenti organizzativi/normativi/ambientali che l'azienda dovesse affrontare.

Le attività della l'Organizzazione sono state analizzate e i processi sono stati suddivisi in:

- Processi di supporto
- Processi Ordinari
- Processi Critici
- Processi Vitali

Elencati in ordine crescente di importanza per l'Organizzazione, i tempi ed il punto di ripristino vengono indicati nella tabella seguente:

Tipo di Processo	**RTO**	**RPO**
Vitale	12 h	6 h
Critico	24 h	12 h
Ordinario	48 h	24 h
Di Supporto	72 h	24 h

3 PROCESSO DI GESTIONE DELLA CONTINUITÀ OPERATIVA

Il processo di continuità operativa è strutturato nelle seguenti fasi:

- **Analisi,** del contesto, dell'impatto sul business (Business Impact Analysis), delle minacce, dei rischi;
- **Progettazione**, che ha l'obiettivo di identificare e selezionare le appropriate strategie e tattiche per determinare il modo in cui saranno raggiunti gli obiettivi di continuità operativa e il recupero dell'operatività a seguito del verificarsi di eventi avversi;
- **Implementazione**, fase in cui vengono messe in atto le strategie e le tattiche e viene attivato il processo di sviluppo della continuità operativa;
- **Verifica** che, attraverso attività di test, esercitazioni, valutazioni di performance e revisioni di audit, conferma che il Programma di continuità operativa soddisfi gli obiettivi stabiliti e che il PCO/BCP sia adatto allo scopo.

Il Piano di Continuità Operativa (PCO/BCP) indica le aree coinvolte nella Continuità Operativa, identifica le persone da attivare durante l'emergenza, dettaglia le attività, i ruoli e i compiti, descrive le relazioni tra le diverse aree, definendo le procedure di supporto ai diversi livelli di operatività.

Il PCO/BCP fornisce precise istruzioni che consentono il governo dell'Organizzazione nelle situazioni di incidente, emergenza e crisi definendo la struttura, le responsabilità e la sequenza temporale di esecuzione delle attività necessarie a fronteggiare l'evento avverso fino a ripristinare la piena operatività. Inoltre, il PCO/BCP prevede i tempi e le responsabilità per l'attivazione dei piani tecnici di ripristino delle varie componenti necessarie all'operatività.

L’architettura predisposta per la Continuità Operativa prevede un piano di gestione della crisi che considera la possibilità che un evento avverso di qualunque genere possa causare l’indisponibilità di una delle componenti necessarie ad erogare i servizi o a realizzare i propri prodotti; in questa prima fase sono state individuate in:

- Indisponibilità del personale (Loss of people)
- Indisponibilità degli immobili (Loss of building)
- Indisponibilità delle infrastrutture (Loss of infrastrutture)
- Indisponibilità dell ‘IT (Loss of IT)
- Indisponibilità di fornitori critici (Loss of Supplier)

Per ognuna delle componenti è stato predisposto un piano di recupero specifico RP – Recovery Plan.

Il presente PCO/BCP comprende 4 piani di recupero (recovery plan):

- Piano di recupero del personale - HR RP
- Piano di recupero degli immobili - BU RP
- Piano di recupero delle infrastrutture - IN RP
- Piano di recupero dell’IT - DR RP
- Piano di recupero dei fornitori critici – CS RP

Considerando che il PCO/BCP è un documento che nasce per essere utilizzato in situazioni di forte stress (a seguito di un incidente o di un evento critico), è necessario che abbia determinate caratteristiche che ne supportino la consultazione e l'utilizzo.

I piani di gestione della crisi e di recupero che compongono il PCO/BCP sono:

- **diretti**, ovvero in grado di fornire direzioni chiare, orientate all'azione e basate sul tempo, consentendo un rapido accesso alle informazioni di supporto pertinenti;
- **adattabili**, ovvero tali da consentire all'organizzazione di rispondere a una vasta gamma di incidenti gravi, compresi quelli che l'organizzazione potrebbe non aver previsto;
- **concisi**, ovvero che contengono esclusivamente una guida delle azioni da intraprendere ed alle informazioni / strumenti che serviranno alle risorse durante un evento;
- **aggiornati**, ovvero che contengono informazioni attuali e applicabili al team che le dovrà utilizzare.

Il Piano di Continuità Operativa copre, inoltre, tutte le fasi della risposta a un evento avverso, da quella iniziale fino alla ripresa delle normali attività.

4 LIVELLI DI OPERATIVITÀ AZIENDALE E RUOLI E RESPONSABILITÀ

L'Organizzazione ha deciso di operare classificando lo stato di operatività in 4 livelli:

- Livello 1 – verde **NORMALE**
- Livello 2 – giallo **INCIDENTE**
- Livello 3 – arancio **EMERGENZA**
- Livello 4 – rosso **CRISI**

Ad ogni stato di operatività corrisponde una diversa organizzazione.

4.1 Livello 1 - Verde - Condizioni di operatività NORMALE

Al livello 1 l'Organizzazione opera nel rispetto dell'organigramma e delle procedure previste.

Sintesi operatività:

- Ruoli e responsabilità – Come previsto in organigramma
- Risorse coinvolte – Tutte come da operatività normale
- Processi impattati e procedure – Tutti i processi e tutte le procedure come previsto dal sistema di gestione della Qualità.
- Attività – Ordinarie

4.2 Livello 2 - Giallo - Operatività durante un INCIDENTE

Al livello 2 l'Organizzazione opera nel rispetto dell'organigramma per tutte le attività / componenti non coinvolte direttamente nell'incidente, mentre, per la/le componenti direttamente coinvolte viene attivato il Responsabile del Piano di Recupero che sarà responsabile di eseguire tutti i passi fino al ripristino delle condizioni di operatività "normale" secondo quanto indicato nell'apposita scheda operativa riportata nel capitolo 8.

Sintesi operatività:

- Ruoli e responsabilità – Responsabile del Piano di recupero della componente coinvolta nell'incidente
- Risorse coinvolte – Responsabile e risorse previste nel piano
- Processi impattati e procedure – Esercizio del piano di recupero.
- Attività – Operatività modificata secondo le esigenze del piano di recupero

4.3 Livello 3 - Arancio - Operatività in EMERGENZA

Al livello 3 l'Organizzazione opera ponendo in esercizio il piano di emergenza che prevede una modifica della normale catena di comando. Vengono attivati il responsabile del piano di emergenza ed i responsabili dei piani di recupero.

Il Responsabile del piano di emergenza allerta il Comitato di Crisi.

Il responsabile del piano di emergenza ha il compito di coordinare le attività di recupero e di mantenere il contatto con il Comitato di Crisi preventivamente allertato.

Il Responsabile del Piano di Emergenza sarà responsabile di tutte le fasi fino al ripristino delle condizioni di operatività "normale" secondo quanto previsto nella apposita scheda operativa riportata nel capitolo 9.

Sintesi operatività:

- Ruoli e responsabilità – Responsabile del Piano di Emergenza – Responsabili dei piani di recupero ed il Comitato di Crisi viene preventivamente allertato
- Risorse coinvolte – Responsabile del piano di emergenza, responsabili dei piani di recupero, risorse previste nei piani
- Processi impattati e procedure – Esercizio del piano di emergenza.
- Attività – Operatività modificata secondo le esigenze del piano di emergenza

4.4 Livello 4 - Rosso - Operatività in CRISI

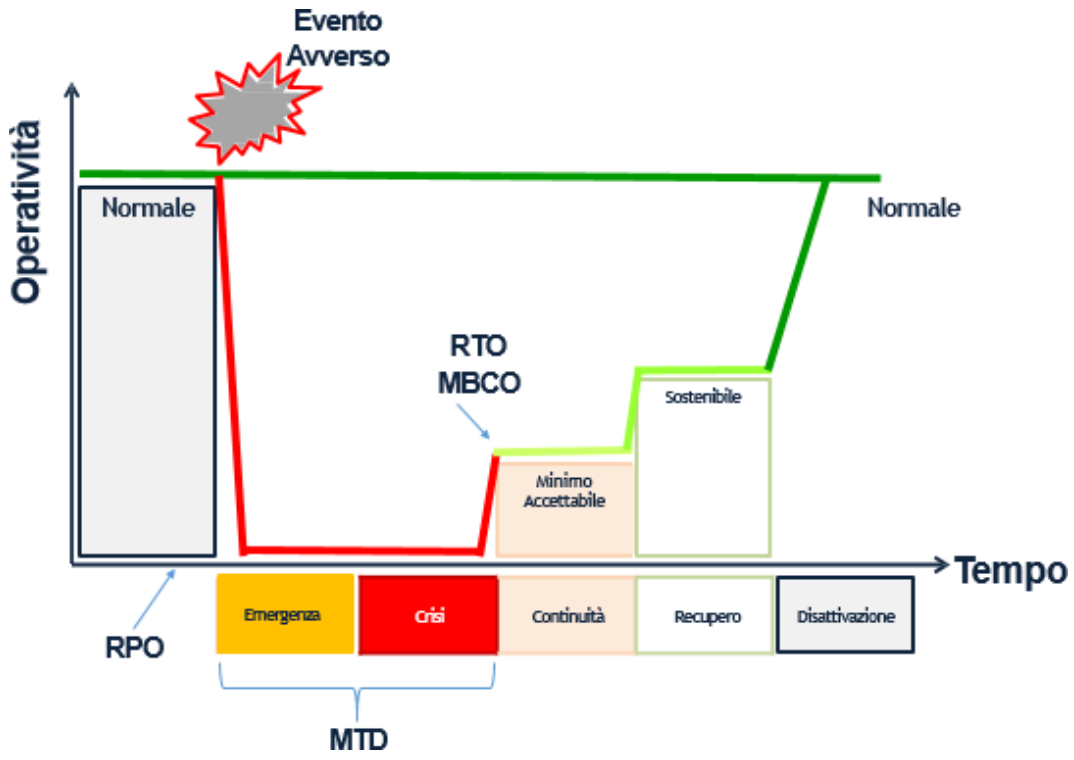
Al livello 4 l'Organizzazione opera in stato di crisi, il governo delle attività e dell'Organizzazione passa al Comitato di Crisi che attiva:

- Responsabile del piano di emergenza
- Responsabili dei paini di recupero
- Responsabile finanziario
- Responsabile della comunicazione

Il Comitato di Crisi sarà responsabile di tutte le attività fino al ripristino delle condizioni di operatività "normale" secondo quanto previsto nella apposita scheda operativa riportata nel capitolo 10.

Sintesi operatività:

- Ruoli e responsabilità – Comitato di Crisi
- Risorse coinvolte – Tutte quelle previste nel Piano di Continuità
- Processi impattati e procedure – Esercizio del piano di continuità.
- Attività – Operatività modificata secondo le esigenze del piano di continuità


Evento
Avverso
Operatività
Normale
Normale
RTO
MBCO
Sostenibile
Minimo
Accettabile
Tempo
RPO
Emergenza
Crisi
Continuità
Recupero
Disattivazione
MTD

5 ASSESSMENT DEI REQUISITI E BUSINESS IMPACT ANALYSIS

5.1.1 Analisi del contesto

Per eseguire l'analisi di contesto l'organizzazione determina i fattori esterni ed interni rilevanti per il proprio sistema di gestione della Continuità Operativa.

La valutazione del contesto esterno include i seguenti fattori:

- l'ambiente politico, giuridico e normativo sia internazionale, nazionale, regionale o locale;
- l'ambiente sociale e culturale, finanziario, tecnologico, economico, naturale e competitivo, a livello internazionale, nazionale, regionale o locale;
- impegni e relazioni della catena di fornitura (supply chain);
- considerazione di studi interni sui rischi, tenendo conto di altri sistemi di gestione delle informazioni pertinenti e più in generale di qualsiasi informazione proveniente dalla gestione della conoscenza;
- fattori chiave e tendenze che hanno un impatto sugli obiettivi e sul funzionamento dell'organizzazione;
- relazioni con, e percezioni e valori di, parti interessate al di fuori dell'organizzazione.

La valutazione del contesto interno include i seguenti fattori:

- prodotti e servizi, attività, risorse, partnership, catena di fornitura (supply chain) e rapporti con le parti interessate;
- le capacità, intese in termini di risorse e conoscenza (ad esempio capitale, tempo, persone, processi, sistemi e tecnologie);
- sistemi di informazione, flussi di informazioni e processi decisionali (sia formali che informali);
- parti interessate all'interno dell'organizzazione;
- politiche e obiettivi e le strategie che sono in atto per raggiungerli;
- opportunità future e priorità aziendali;
- percezioni, valori e cultura;
- standard e modelli di riferimento adottati dall'organizzazione; e
- strutture (ad esempio governance, ruoli e responsabilità).

Nella gestione del proprio Sistema di gestione della continuità operativa l'Organizzazione garantisce che le esigenze e le aspettative delle parti interessate siano prese in considerazione, sia quelle esplicite che quelle implicite.

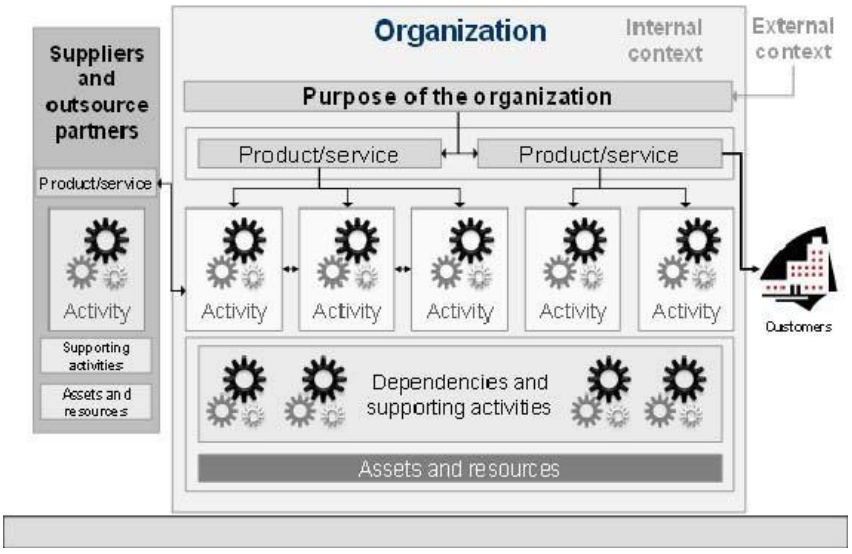
Tra le parti interessate si prendono in considerazione sia quelle primarie senza il cui supporto l'organizzazione cesserebbe di esistere (stakeholder), sia di coloro che hanno un interesse nell'organizzazione,

come ad esempio i media, i cittadini in prossimità delle strutture aziendali, i concorrenti ecc.

Individuare tutte le parti interessate interne ed esterne da considerare è fondamentale in particolare per quanto riguarda i processi di comunicazione, ad esempio, potrebbe essere necessario comunicare con tutte le parti interessate a seguito di un incidente di disturbo, ma potrebbe non essere opportuno comunicare con tutte le parti interessate durante tutte le fasi del programma di continuità operativa in presenza di una emergenza o una crisi.

5.1.2 BIA (Business Impact Analysis) ed Analisi dei Rischi

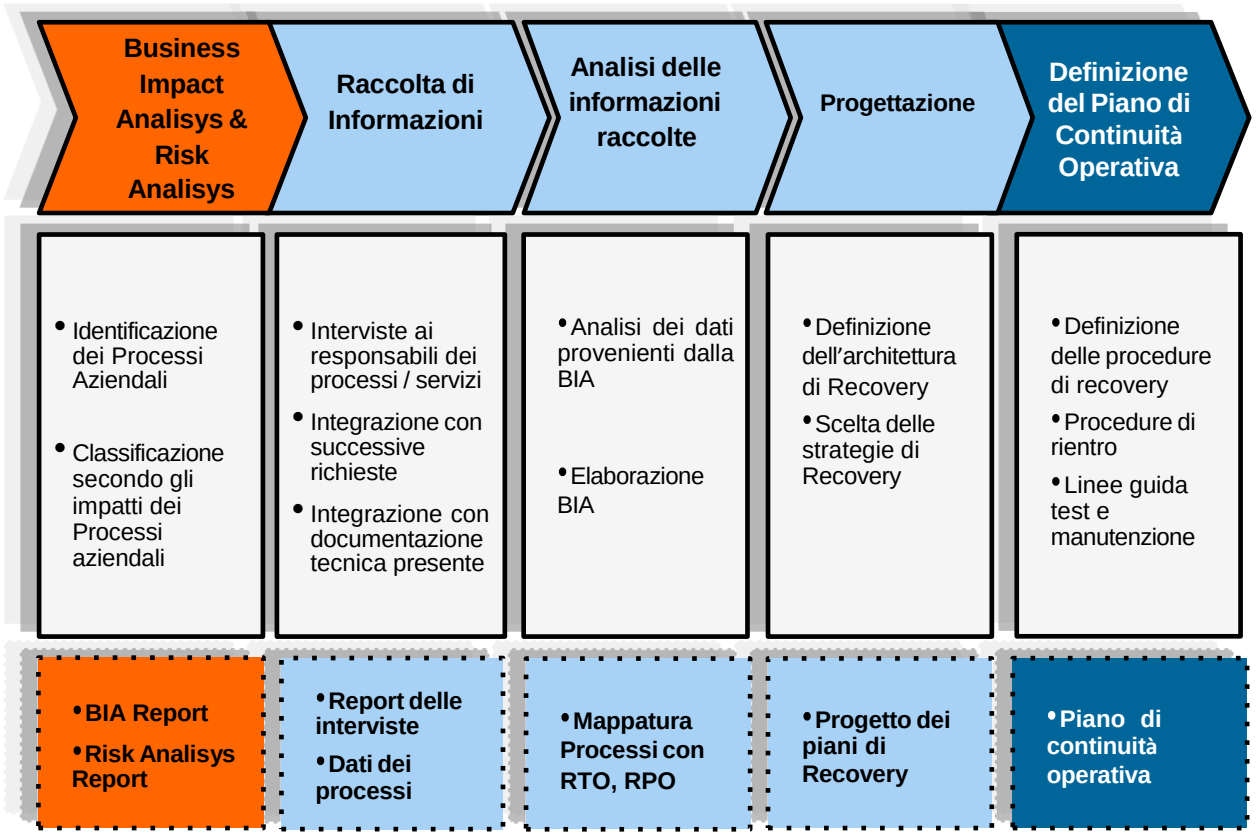
La Business Impact Analysis (BIA) è la valutazione dell'impatto sul business in caso di eventi di rilievo che possono compromettere le attività aziendali e l'erogazione dei servizi. Al fine di indirizzare appropriate soluzioni di Business Continuity, vengono identificati i requisiti di ripartenza dei servizi.



L' Organizzazione realizza la Business Impact Analysis con l'obiettivo di:

- censire i processi rilevanti per il business aziendale;
- identificare gli impatti legati all'indisponibilità del processo;
- identificare i tempi di ripristino compatibili con quanto previsto a livello contrattuale e/o normativo;
- identificare i processi maggiormente critici;
- classificare tutti i processi individuati;
- identificare le priorità con la quale i processi hanno la necessità di essere ripristinati.

La Business Impact Analysis riporta principalmente l'analisi dei processi di business e l'individuazione delle attività critiche utilizzando i parametri di valutazione che tengono conto di vincoli a livello normativo, vincoli contrattuali con i clienti, rilevanza del servizio/attività per il business aziendale, rilevanza strategica del servizio/attività per l'azienda.



L'analisi dell'impatto aziendale include:

a) l'identificazione delle attività che supportano la fornitura dei prodotti e dei servizi chiave dell'organizzazione;

b) valutare i potenziali impatti nel tempo delle interruzioni derivanti da eventi incontrollati e non specifici su queste attività. Nel valutare gli impatti, l'organizzazione deve principalmente considerare quelli relativi ai propri scopi e obiettivi di business e alle parti interessate, questi possono includere:

1) effetti negativi sul personale o sul benessere pubblico,

2) conseguenze di violazione dei doveri statutari o dei requisiti normativi,

3) danno alla reputazione,

4) redditività finanziaria ridotta,

5) deterioramento della qualità del prodotto o del servizio e

6) danno ambientale;

c) la stima del tempo necessario per rendere inaccettabili gli impatti associati all'interruzione delle attività dell'organizzazione;

d) la valutazione del tempo necessario per riprendere, ad un livello minimo accettabile le attività dell'organizzazione

e) la considerazione di tutti i tempi necessari identificando le dipendenze e le risorse di supporto, includendo i fornitori, i partner esterni e le altre parti interessate

La BIA è stata realizzata raccogliendo le informazioni da:

– interviste;

– questionari;

– altre fonti interne ed esterne.

La BIA viene aggiornata con le informazioni fornite dalle strutture aziendali coinvolte e resa disponibile all'azienda per la predisposizione dei piani di Recovery.

Il Risk Assessment è finalizzato alla prevenzione e al contrasto delle minacce che possono colpire gli asset aziendali provocandone, tra gli altri impatti, l'indisponibilità per un periodo più o meno prolungato. Con l'effettuazione del Risk Assessment, L'Organizzazione sì propone di proteggere il valore aziendale, perseguire gli obiettivi aziendali e gestire i rischi che potrebbero comportare la perdita di riservatezza, integrità, disponibilità e conformità dei servizi / processi aziendali. Il processo di gestione dei rischi di L'Organizzazione descrive come i rischi sono identificati, analizzati, valutati, trattati, monitorati e aggiornati con le relative responsabilità.

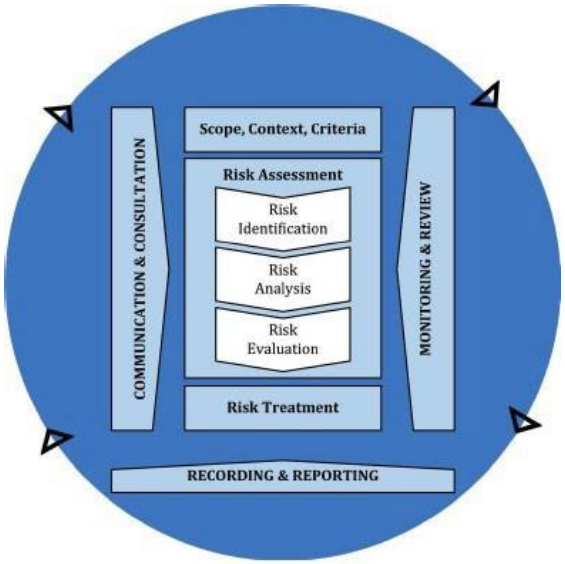


Figure 4 — Process

La decisione sul trattamento dei rischi individuati è basata sulla valutazione del giusto equilibrio fra il rispetto delle norme cogenti, le necessità di business ed il costo delle tecnologie di sicurezza. Si declina nelle classiche opzioni di trattamento dei rischi:

- mitigare
- accettare
- evitare
- trasferire.

Sulla base delle decisioni assunte, viene compilato il cosiddetto Piano di Trattamento dei Rischi, che contiene le modalità che L'Organizzazione ha deciso di adottare per trattare i rischi individuati. L'Organizzazione aggiorna periodicamente, e monitora in modo sistematico, il Piano di Trattamento dei Rischi.

L'analisi dei rischi viene effettuata ad intervalli pianificati ed anche ad ogni cambiamento significativo, viene eseguita per ogni nuova iniziativa (processi, servizi o progetti). L'analisi dei rischi tocca tutti gli aspetti impattati nella sicurezza e nella sicurezza delle informazioni logici, fisici, tecnici ed organizzativi.

Il processo implementato tratta gli aspetti seguenti:

- determinazione dei criteri per l'accettazione del rischio;
- identificazione dei livelli di rischio accettabili;
- analisi dei rischi affronta:

- le minacce specifiche che possono essere descritte come eventi o azioni che potrebbero, causare un impatto sulle risorse, ad es. minacce come incendio, alluvione, interruzione di corrente, perdita di personale, assenteismo del personale, virus informatici e guasti all'hardware; e
- le vulnerabilità che possono verificarsi come punti deboli all'interno delle risorse e possono essere sfruttate dalle minacce, ad es. singoli punti di errore, inadeguatezza nella protezione antincendio, resilienza elettrica, livelli di personale, sicurezza IT e resilienza IT.

5.1.3 Strategia di Continuità Operativa

La strategia di continuità operativa è basata sui risultati dell'analisi dell'impatto aziendale e della valutazione del rischio. L'obiettivo della strategia di continuità operativa è ridurre l'impatto complessivo delle interruzioni accorciando il periodo di interruzione e riducendone l'intensità a livelli accettabili.

L'organizzazione ha determinato le opzioni strategiche per:

a) la protezione delle attività prioritarie

Questi possono essere mirati a rimuovere i rischi per l'attività, a trasferire le attività a terzi e cessare o modificare l'attività se sono disponibili valide alternative.

Le opzioni per proteggere le attività prioritarie dovrebbero essere selezionate in base a:

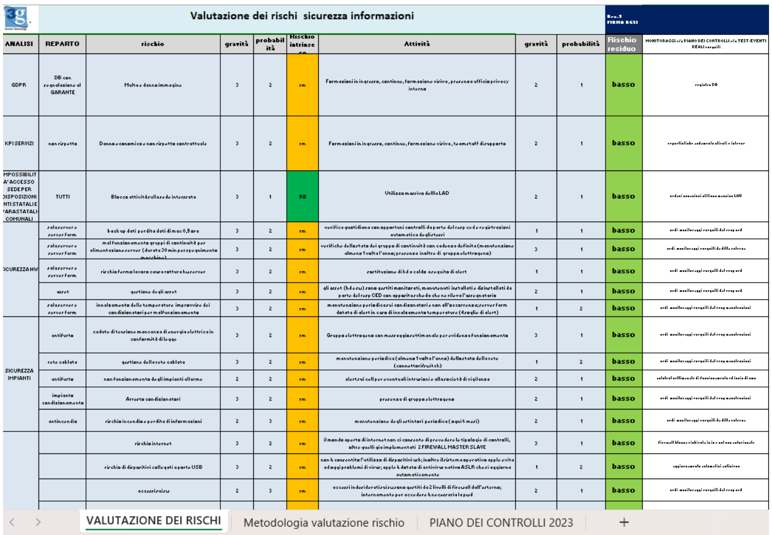
1. le vulnerabilità percepite dell'attività;
2. il costo delle misure rispetto ai benefici stimati;
3. l'urgenza dell'attività
4. la fattibilità e l'idoneità complessive dell'opzione.

Le opzioni di continuità possono includere:

1) il trasferimento dell’attività;
2) il trasferimento o riallocazione delle risorse;
3) i processi alternativi e capacità inutilizzata;
4) la sostituzione delle risorse e delle competenze;
5) l’adozione di una soluzione temporanea, come ad esempio, adottare per alcune attività, un metodo di lavoro diverso che fornisca risultati accettabili per un periodo di tempo limitato. È possibile che la soluzione alternativa richieda più tempo e / o lavoro più intenso (ad esempio un'operazione manuale anziché un sistema automatico). Per questi motivi, la soluzione alternativa dovrebbe essere considerata solo per estendere il periodo prima che sia necessario un ritorno alla normalità;

Modello analisi dei rischi esempio

ESTRATTO TOOL Organizzazione



Modello BIA esempio

TIPOLOGIA IMPATTO	BASSO	MEDIO	ALTO
Economico	*Interruzione del servizio con impatti economici trascurabili*	*Interruzione del servizio con impatti economici che possono compromettere la redditività del servizio*	*Interruzione del servizio con impatti economici che possono compromettere la stabilità finanziaria dell'azienda*
Reputazionale	*Interruzione di una componente del servizio senza impatti percepiti dal cliente*	*Interruzione di servizio per un tempo ridotto e nei limiti previsti dagli SLA*	*Interruzione di servizio che comporta un mancato raggiungimento delle soglie fissate con gli SLA*
Operativo	*Indisponibilità di una componente del servizio che può essere ripristinata con misure ordinarie*	*Indisponibilità di una componente del servizio che può essere ripristinata con l'impiego di misure straordinarie*	*Indisponibilità del servizio che richiede l'attivazione di procedure di emergenza e ripristino e/o l'impiego di risorse economiche extra*
Normativo	*Mancato rispetto di obblighi di compliance che comportano adempimenti minori o sanzioni di lieve entità*	*Mancato rispetto di obblighi di compliance che comportano adempimenti onerosi o sanzioni economiche rilevanti*	*Mancato rispetto di obblighi di compliance che possono comportare il fermo del servizio da parte delle autorità*

Servizio **Core business**

Processi	SLA	Impatti	2h	4h	8h	12h	24h	48h	72h	TBD	RTO	MBCO
Processo 1	TBD	*Economico*	B	B	B	M	M	A	A	A	12h	TBD
		Reputazionale	B	B	B	A	A	A	A	A		
		Operativo	B	B	B	B	M	A	A	A		
		Normativo	B	B	B	B	B	B	B	B		
Processo 2	TBD	*Economico*	B	B	B	B	M	M	A	A	48h	TBD
		Reputazionale	B	B	B	B	B	B	B	B		
		Operativo	B	B	B	B	M	M	M	A		
		Normativo	B	B	B	B	B	A	A	A		
Processo 3	TDB	*Economico*	B	B	B	B	B	B	B	B	48h	TBD
		Reputazionale	B	B	B	M	M	A	A	A		
		Operativo	B	B	M	M	M	M	M	A		
		Normativo	B	B	B	M	M	M	M	M		

6 GESTIONE DELLA CONTINUITÀ

Di seguito lo schema del modello applicato

<table>
<tr><td>Normale Operatività</td><td colspan="2">In questa fase occorre svolgere le attività necessarie per mantenere la validità del Piano di Continuità. Ad esempio: le simulazioni pianificate, le verifiche periodiche, la gestione dei cambiamenti, la revisione in relazione alle mutate esigenze a cui deve rispondere.</td></tr>
<tr><td rowspan="3">Emergenza</td><td>Valutazione</td><td>In caso di interruzione (totale o parziale) dell’operatività dei servizi erogati, è la fase nella quale si deve decidere se attivare il ripristino o se è sufficiente avviare le usuali procedure interne per riportare alla normalità l’operatività.
Prevede la documentazione dei criteri utilizzati e, se possibile, una stima del danno prodotto dall’interruzione del servizio.</td></tr>
<tr><td>Ripristino</td><td>E’ la fase durante la quale vengono svolte le attività di riattivazione e di ricostruzione del sistema informativo.</td></tr>
<tr><td>Normalizzazione</td><td>E’ la fase durante la quale viene controllata la validità del sistema informativo ripristinato, con particolare attenzione al contenuto delle basi dati e al funzionamento della connettività e la rete di utenza.</td></tr>
<tr><td>Esercizio Provvisorio</td><td colspan="2">E’ la fase durante la quale i servizi informatici sono erogati da un Sito Secondario.
In tale periodo è in corso la risoluzione nel Sito Primario della situazione di emergenza che ha innescato l’avvio del ripristino. In questa fase vengono erogati i servizi indispensabili per mantenere in vita l’azienda/organizzazione.
La durata di questa fase è stimabile nei tempi stabiliti, e dipende dal tempo necessario per rendere nuovamente operativo il Sito Primario.
(tale durata può essere sottoposta a limitazioni dovute a vincoli normativi o legali (ad es.: legislazione vigente o questioni relative ad eventuali coperture assicurative).</td></tr>
</table>

Rientro	Dopo che è stata risolta l'emergenza nel Sito Primario, è la fase durante la quale l'erogazione del servizio informativo interrotto viene trasferita nuovamente dal Sito Secondario al Sito Primario. Il rientro avviene in modo adeguatamente pianificato, concordato e preventivamente collaudato.

Allarme

L' allarme verrà attivato nel caso di:

- Impatto ambientale, Impatto sulla Sede Fisica o Interruzione delle forniture di Energia elettrica o servizi telefonici se non è stato possibile avere informazioni precise sui tempi di ritorno alla normalità o se le previsioni indicano tempi di soluzione superiori a 2 ore.
- Guasti agli impianti tecnologici, guasti in sala macchine o alle attrezzature di rete nel caso in cui sia prevista una interruzione del servizio informatico superiore a 2 ore.
- Perdita o inconsistenza dei dati e/o problemi al software solo dopo aver fatto una valutazione di dettaglio del problema e delle possibili soluzioni con gli specialisti ed aver verificato che la risoluzione del problema potrebbe richiedere tempi superiori a quanto stabilito dall'RPO.

L' allarme può essere interrotto in qualsiasi momento se la situazione dovesse essere recuperata; in questo caso è necessario procedere con le attività prevista nel paragrafo, oppure può evolvere ad una situazione di emergenza effettiva mediante la Dichiarazione di Livello di operatività diverso da normale.

Valutazione a seguito Allarme

Ha l'obiettivo di procedere ad una valutazione dello scenario se procedere al ripristino e dare l'avvio alle procedure di Recupero del Sito Primario (dipendenti dallo scenario individuato).

In caso di annullamento dell'allarme, la situazione di Emergenza viene chiusa in quanto la situazione verrà risolta tramite le procedure di Recupero.

Dichiarazione stato di livello diverso da normale

È l'atto ufficiale con il quale si notifica lo stato di livello diverso da normale a:

- Al personale interno;
- Alle società con cui è stato stipulato un Contratto di Servizio
- agli enti con cui è stato stipulato un eventuale Accordo di Soccorso
- agli enti esterni ai quali si erogano servizi impattati dall'emergenza
- alle autorità competenti, qualora ve ne sia l'obbligo/la necessità

Ripristino

Durante questa fase vengono svolte tutte le attività necessarie alla ricostruzione dei Sistemi ed eventualmente, dell'attivazione di posti lavoro di emergenza nella configurazione che prevede l'uso del sito secondario.

Per una più efficiente suddivisione ed attuazione dei compiti, si prevede che il Gruppo di Intervento Ripristino Sistemi (GI-RS) venga articolato a livello di ambiente, per garantire una maggiore specializzazione e una scomposizione in sottofasi più precisa. Pertanto vengono individuati i seguenti sottogruppi:

- Ambiente operativo;
- Ambiente Rete e TLC.
- Posti di Lavoro

Come per la fase di Valutazione, anche questa fase deve essere accuratamente documentata secondo quanto previsto dalla apposita modulistica messa a supporto; tali documenti devono quindi essere archiviati per eventuali attività di audit successive.

N.B.: nessuna attività eseguita in fase di Ripristino deve impedire l'eventuale ripartenza presso il sito primario qualora questa possa essere attuata.

Normalizzazione

Durante questa fase vengono svolte le attività necessarie alla verifica che gli ambienti informatici ricostruiti presso il sito secondario siano stati correttamente ripristinati per le varie componenti interessate dall'intervento come ad esempio:

- Componente Infrastrutturale (apparati HW, linee TLC, sistemi operativi, prodotti SW)
- Componente Applicativa (completezza e allineamento delle basi dati)
- Utenza finale (connettività; utilizzabilità dei servizi)

In fase di Normalizzazione si individua il livello di perdita dei dati, cioè il momento temporale, precedente il blocco dei servizi, oltre il quale occorre rieseguire le operazioni che risultano andate perdute.

Le attività da svolgere nella fase sono documentate in dettaglio nel Manuale Tecnico. All'interno di tale documento, sono presenti i criteri da utilizzare per la scelta della opportuna versione di Base Dati da cui partire per l'attività di Normalizzazione.

N.B.: nessuna attività eseguita in fase di Normalizzazione deve impedire l'eventuale ripartenza presso il sito primario qualora questa possa essere attuata.

Esercizio provvisorio

E’ la fase durante la quale i servizi sono erogati da un Sito secondario.

In tale periodo è in corso la risoluzione nel Sito primario della situazione di emergenza che ha innescato l’avvio del ripristino. In questa fase vengono erogati i servizi indispensabili per mantenere in vita l’azienda / organizzazione.

La durata di questa fase è stimabile nei tempi stabiliti, e dipende dal tempo necessario per rendere nuovamente operativo il Sito primario.

(tale durata può essere sottoposta a limitazioni dovute a vincoli normativi o legali ad es.: legislazione vigente o questioni relative ad eventuali coperture assicurative).

Rientro

Dopo che è stata risolta l’emergenza nel Sito primario, è la fase durante la quale l’erogazione del servizio informativo interrotto viene trasferita nuovamente dal Sito secondario al Sito primario. Il rientro avviene in modo adeguatamente pianificato, concordato e preventivamente collaudato.

7 SCENARI DI INDISPONIBILITÀ ANALIZZATI E PIANI DI RECOVERY

Di seguito una tabella che contiene un esempio di scenari di indisponibilità valutati

MINACCIA	RISORSA IMPATTATA	CLASSE SCENARIO
• Crollo strutturale, terremoto, frana • Incendio • Tromba d'aria, tempesta di neve • Inondazione • Contaminazione ambientale, • Atti di terrorismo, sabotaggio	• Uffici • ICT • Produzione	**A-Inaccessibilità dei locali**
• Blocco, guasto, malfunzionamento grave di sistemi, reti, infrastrutture, impianti, ecc. • Interruzione erogazione energia elettrica, gas, acqua, combustibili • Grave perdita e corruzione dati, frode interna • Attacchi esterni ICT • Indisponibilità di forniture essenziali per i sistemi ICT	• Rete (linee, apparecchiature, software rete) • Infrastrutture IT (hardware, software base, database) • Sistemi applicativi • Sistemi gestionali ICT • Servizi infrastrutturali • Dati e documentazione	**B-Interruzione e disfunzione dei sistemi ICT e delle infrastrutture**
• Fine erogazione delle forniture (fallimento, rescissione contratto) • Mancato approvvigionamento (problemi di logistica del fornitore)	• Fornitura materiali • Fornitura servizi • Elettricità, acqua, telefono	**C- Indisponibilità di forniture essenziali per i processi**
• Azioni sindacali, sciopero • Licenziamento, dimissioni • Malattie, infortuni • Epidemia • Blocco dei trasporti	• Responsabili ICT, Security, Safety • Responsabili altre funzioni • Personale specialistico • Personale operativo • Personale di produzione	**D - Indisponibilità di personale essenziale**

7.1.1 Indisponibilità del personale (Human Continuity Plan – HCP)

Per rispondere all'emergenza della mancanza di personale (quando un evento causa la mancanza contemporaneamente di tutto il personale di un ufficio o un'area come uno sciopero, una pandemia, una difficoltà ad arrivare sul posto di lavoro, ecc.) la Organizzazione ha una mappa delle competenze che tiene a disposizione e di facile reperimento per poter chiamare e sostituire il personale mancante con altro disponibile. Tale documento contiene anche tutti i riferimenti per rintracciarli. Esiste un organigramma da attivare in caso di crisi che permette di individuare immediatamente i responsabili da chiamare ed eventualmente come scalare al livello successivo.

Inoltre, per ovviare alla eventuale mancanza di competenza sul lavoro da svolgere, una misura applicata è la ridondanza delle competenze con formazione e training on the job.

La stessa misura viene adottata nel selezionare più fornitori esterni con competenze analoghe.

7.1.2 Indisponibilità degli immobili (Building Recovery Plan – BUPR)

Per rispondere alla mancanza di disponibilità della build (quando un evento causa l'impossibilità di accesso alle strutture fisiche dell'azienda come interruzione delle vie di accesso, ecc) la L'Organizzazione ha attivato un accordo quadro LAD (RUMOO1AP/20) che copre il comparto operativo e direzionale e che consente (vedi es. PANDEMIA- TERREMOTO) di non avere interruzioni nel business.

7.1.3 Indisponibilità delle Infrastrutture (Infrastructure Recovery Plan – INPR)

Per rispondere alla mancanza di disponibilità delle infrastrutture (quando un evento causa l'indisponibilità di corrente elettrica, acqua, gas, fonti di energia alternativa, smaltimento rifiuti, ecc) è fondamentale avere nella disponibilità aziendale dei siti secondari necessari allo svolgimento del servizio minimo (comprese macchine, attrezzature, spazi, ecc.). Tale/i sito/i devono essere sempre pronti ad operare. Per accertarsene devono essere eseguiti test e verifiche reali.

Una misura applicata è che la L'Organizzazione ha sottoscritto degli Indisponibilità dell'infrastruttura è la stipula di un accordo quadro LAD (RUMOO1AP/20)

(IT Recovery Plan – IRP)

Per rispondere alla mancanza di disponibilità dell'IT (in tutto o in parte), l'azienda L'Organizzazione ha predisposto un piano di DR che prevede il salvataggio di tutti i dati, in particolare quelli del server vengono "backuppati" ogni 24 ore su un NAS con dischi in Raid 1+0 e quotidianamente vengono nuovamente salvati su sede aziendale back up.

E' sempre presente o reperibile H24 7/7 IT fisico per tale motivo, in caso di problemi su perdita di dati o loro integrità si può fare un ripristino di tutti i lavori nell'arco di pochi minuti.

Il CED è dotato di un UPS costantemente testato e sufficiente al ripristino come previsto dal piano di Continuità Operativa.

7.1.4 Indisponibilità deli fornitori critici (CS Recovery Plan – CRPR)

Per rispondere alla mancanza di disponibilità dei fornitori critici abbiamo creato una ridondanza su più sedi e richiesto alle società di assicurarci anche la possibilità che i loro dipendenti dedicati alle nostre attività possano lavorare in lad.

8 PCO/BCP - LIVELLO 25 - CONDIZIONI DI NORMALE

A livello **NORMALE** la L'Organizzazione opera nel rispetto di quanto indicato nel proprio sistema di gestione della qualità riportato nel Manuale Integrato, i processi eseguiti sono:

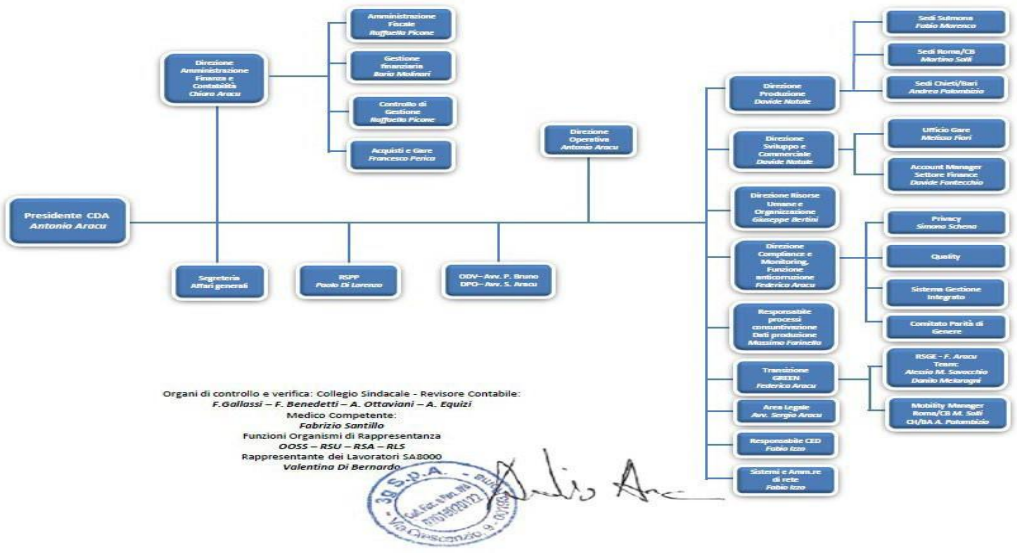
processi primari:

- Amministrazione
- Risorse Umane
- Attività di C.C. BO
- Attività di C.C. Inbound
- Attività di C.C. Outbound
- IT
- Approvvigionamento e valutazione fornitori

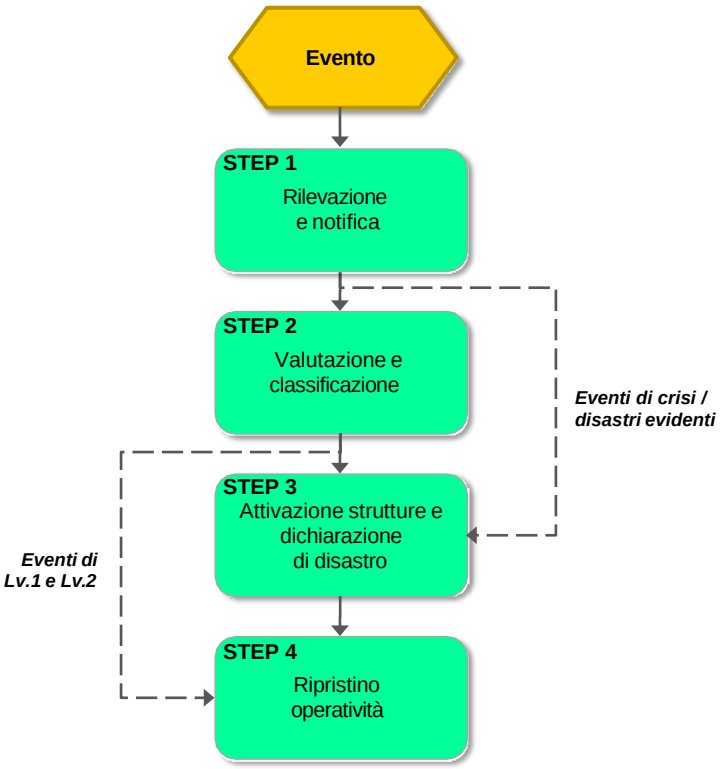
processi di supporto:

- valutazione delle risorse (interne ed esterne) per lo svolgimento di attività aventi influenza sulla operatività aziendale
- gestione delle informazioni e della documentazione,
- monitoraggio delle attività produttive
- verifiche ispettive
- riesame della Direzione,
- gestione delle non conformità reali ed individuazione delle non conformità potenziali e delle opportunità di miglioramento per il miglioramento continuo

Organigramma



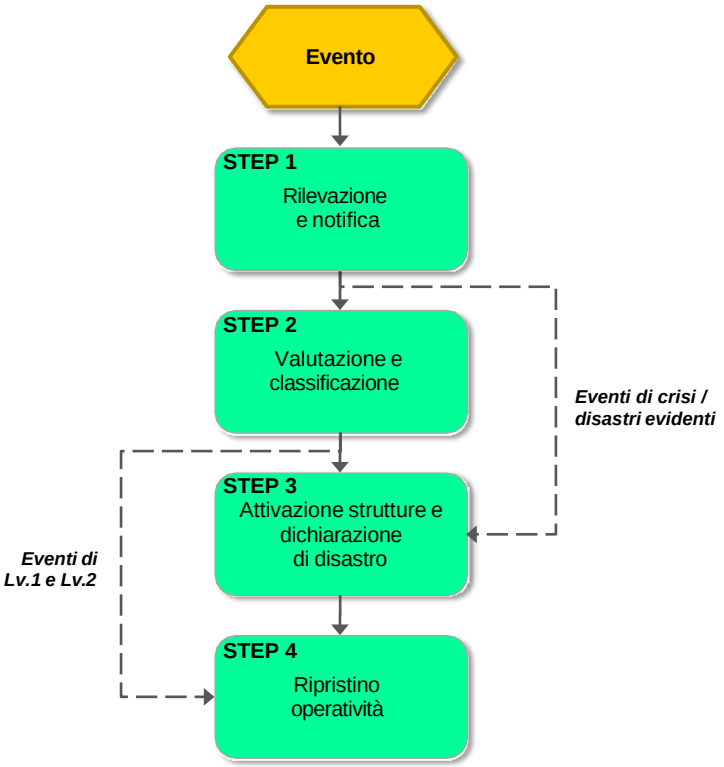
9 PCO/BCP - LIVELLO 26 - CONDIZIONI DI INCIDENTE



RESTO DEL CONTENUTO NON DISPONIBILE NELLA VERSIONE PUBBLICA

DESCRIZIONE DEI PASSI OPERATIVI DA COMPIERE – LISTA DELLE RISORSE COINVOLTE – ECC.

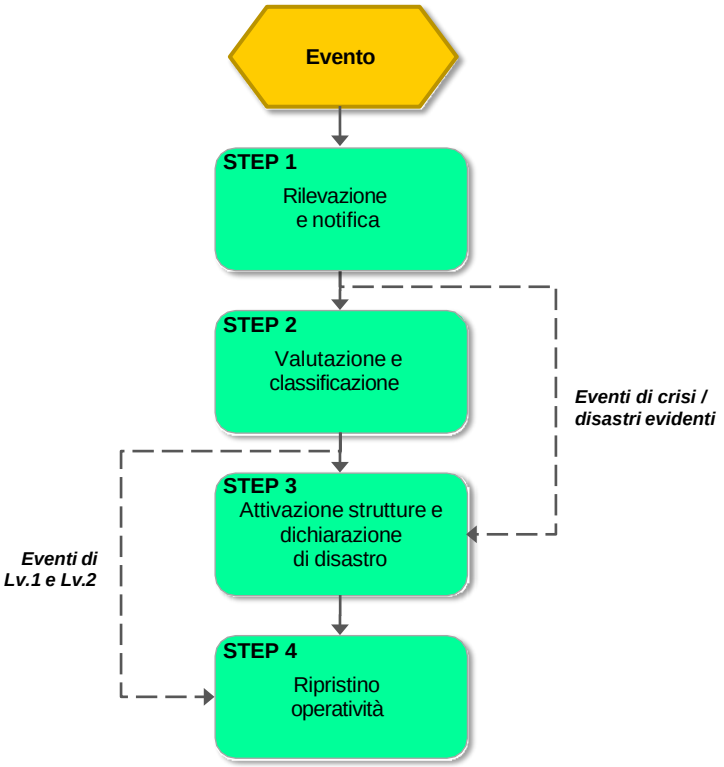
10PCO/BCP - LIVELLO 27 - CONDIZIONI DI EMERGENZA



RESTO DEL CONTENUTO NON DISPONIBILE NELLA VERSIONE PUBBLICA

DESCRIZIONE DEI PASSI OPERATIVI DA COMPIERE – LISTA DELLE RISORSE COINVOLTE – ECC.

11 PCO/BCP - LIVELLO 28 - CONDIZIONI DI CRISI



RESTO DEL CONTENUTO NON DISPONIBILE NELLA VERSIONE PUBBLICA

DESCRIZIONE DEI PASSI OPERATIVI DA COMPIERE – LISTA DELLE RISORSE COINVOLTE – ECC.

Parte integrante del piano è la procedura di BCP/CO DMP017PP/A (ALL. A) (contiene DRP)

Per revisione
Resp. C.O.

Per approvazione
Presidente CDA

12 RIFERIMENTI NORMATIVI

ID	Norma	Descrizione
1	Iso 9001:2015	Sistema di Gestione Qualità
2	Iso 22301:2019	Sistema di Gestione della Continuità Operativa
3	Iso 22313:2020	Guida all'implementazione del Sistema di Gestione della Continuità Operativa

3G S.P.A.	DIREZIONE MONITORING E COMPLIANCE	DMP017PP/A	
POLITICHE E PROCEDURE DEL PERSONALE (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

Procedura BUSINESS CONTINUITY/CO (PBC)

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
2	**31/07/2023**	SINTESI CAMBIAMENTI **AGGIORNAMENTO NORME ISO**	DIREZIONE MONITORING E COMPLIANCE	PRESIDENTE C.D.A.

3G S.P.A.	DIREZIONE MONITORING E COMPLIANCE	DMP017PP/A	
POLITICHE E PROCEDURE DEL PERSONALE (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 📖 INTERNA ▽ ESTERNA

Contenuti

Nome documento	Procedura Business Continuity	Codifica	DMP017PP/A
Ufficio responsabile	Direzione Monitoring e Complince	Data pubblicazione	31/07/2017
Indice revisione	Rev. 2	Data revisione	31/07/2023
Responsabile revisione	RGSI	Responsabile approvazione	Presidente CDA

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017, ISO22301:2019, ISO/IEC27001:2013, ISO37001:2016, ISO45001:2018 SA8000:2014 UNI_PdR 125 2022 ISO 14064-2019 e ISO 50001-2018.

Riservatezza/Avviso di sicurezza

INTRODUZIONE

1 Obiettivi e finalità

3g Spa pone grande attenzione alla Business Continuity (Continuità Operativa) quale elemento cruciale per l'erogazione dei propri servizi nel pieno rispetto di quanto definito anche nei contratti con i Committenti, delle Linee Guida interne e le Procedure di riferimento e, più in generale, in coerenza con le metodologie e gli standard internazionali cogenti / normanti. In tal senso ha sviluppato e mantiene un sistema di Business Continuity, definizione che racchiude in sé un sistema composto da politiche, procedure, mentalità votata alla Continuità Operativa, ovvero un sistema che contempla soluzioni logistiche, organizzative e tecnologiche. Tale sistema è in grado di supportare efficacemente e tempestivamente l'organizzazione a fronte di una situazione di emergenza. La BC fonda i suoi presupposti sulla normativa di riferimento ISO 22301 Business Continuity e negli anni 3g vanta una continuità operativa riscontrabile in ogni tipologia di evento (terremoto, blackout, pandemia per citare alcuni esempi) e segue i principi delle line guida ISO 31000:2018.
L'obiettivo principale del Sistema di Continuità operativa di 3g Spa è quello di garantire che l'organizzazione sia in grado di reagire a fronte di eventi o danni che possano minacciare la sopravvivenza e/o l'immagine aziendale e il controllo dei processi erogati.

2 Campo di applicazione

PROGETTAZIONE, REALIZZAZIONE E GESTIONE DI ATTIVITÀ DI CALL E CONTACT CENTER. PROGETTAZIONE, SVILUPPO E MANUTENZIONE EVOLUTIVA DI SOLUZIONI INFORMATICHE.

3 Ruoli e responsabilità

Alta Direzione CONTROLLO
Direzione Compliance VERIFICA CONFORMITA'
Responsabile continuità operativa APPLICAZIONE E CONTROLLO OPERATIVO
Responsabile continuità operativa tecnica APPLICAZIONE E CONTROLLO TECNICO
Staff operativi APPLICAZIONE DELLE PROCEDURE

4 Procedure

La Procedura Business Continuity di 3gSPA è parte integrante del BCP/PCO e si articola in una serie di policy e procedure di seguito riportate.


3g
Human Technology

3G S.P.A.	AREA MONITORING E COMPLIANCE	DMP006PP	
POLITICHE E PROCEDURE DEL PERSONALE (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

DISASTER RECOVERY PLAN

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIREZIONE MONITORING E COMPLIANCE	PRESIDENTE C.D.A.
4	**21.07.2023**	**AGGIORNAMENTO ISO**		

Contenuti

Nome documento	Procedura Disaster Recovery	Codifica	DMP006PP
Ufficio responsabile	Direzione Monitoring e Compliance	Data pubblicazione	31/07/2017
Indice revisione	Rev. 4	Data revisione	21/07/2023
Responsabile revisione	RSGI	Responsabile approvazione	Presidente C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
4	**21.07.2023**	SINTESI CAMBIAMENTI **AGGIORNAMENTO ISO**	DIREZIONE MONITORING E COMPLIANCE	PRESIDENTE C.D.A.

DISASTER RECOVERY PLAN

1. Scopo e campo di applicazione

Procedura per fronteggiare eventuali situazioni di emergenza provocate da eventi la cui evoluzione può produrre gravi danni per le persone, la sicurezza delle informazioni, la continuità del business aziendale, la continuità dei servizi erogati.

2. Termini e definizioni

Si fa riferimento al glossario ISO 27001 e ISO 22301.
Le responsabilità operative dell'applicazione della presente procedura sono descritte di seguito.

3. Riferimenti

Norme ISO 27001 e ISO 22301.

4. Modalità operative

4.1. Modalità operative

In linea generale la sequenza di azioni previste è la seguente:

- tempestivo riconoscimento dell'evento e della sua natura dannosa;
- Interruzione del danno o sua circoscrizione;
- ripristino delle condizioni pre-evento anche in termini di riassorbimento del danno o quanto meno di un livello accettabile di riassorbimento.

4.2. Soluzioni logistiche

Al fine di tutelarsi a fronte di eventi che possano minacciare la sicurezza dell'azienda, 3g Spa si è dotata di sedi attrezzate con le più moderne e sofisticate misure di sicurezza fisica, quali ad esempio un sistema di controllo accessi, intrusion detection, difesa perimetrale, rilevamento allagamenti e infiltrazioni, antincendio, gruppi di continuità e/o soluzioni alternative.
Inoltre, gli edifici che ospitano le sedi sono costruiti secondo norme antisismiche.
Oltre a quanto sopra descritto, per rispondere in modo adeguato al verificarsi di un evento di tipo disastroso, 3g Spa si è dotata di più sedi di lavoro (sulle quali sono dislocate le macchine e le risorse umane) e di un sito completamente esterno su server farm dedicata in grado di gestire la ripartenza dei servizi in caso di evento disastroso (per i servizi ritenuti critici dall'azienda e per quelli contrattualizzati con i clienti).
Sono inoltre state predisposte situazioni logistiche per "data-room" equipaggiate con work-station, collegamenti con più provider, denaro, strumenti di documentazione.

4.3. Soluzioni tecnologiche

Al fine di tutelarsi a fronte di eventi che possano minacciare la sicurezza dell'azienda, 3g Spa si è dotata di sedi attrezzate con le più moderne e sofisticate misure di sicurezza fisica, quali ad esempio un sistema di controllo accessi, intrusion detection, difesa perimetrale, rilevamento allagamenti e infiltrazioni, antincendio, gruppi di continuità e/o soluzioni alternative.

Inoltre, gli edifici che ospitano le sedi sono costruiti secondo norme antisismiche.
Oltre a quanto sopra descritto, per rispondere in modo adeguato al verificarsi di un evento di tipo disastroso, 3g Spa si è dotata di più sedi di lavoro (sulle quali sono dislocate le macchine e le risorse umane) e di un sito completamente esterno su server farm dedicata in grado di gestire la ripartenza dei servizi in caso di evento disastroso (per i servizi ritenuti critici dall'azienda e per quelli contrattualizzati con i clienti).
Sono inoltre state predisposte situazioni logistiche per "data-room" equipaggiate con work-station, collegamenti con più provider, denaro, strumenti di documentazione.

4.4. Coinvolgimento della clientela

La completa realizzazione della Business Continuity non può prescindere dallo sviluppo di un rapporto di collaborazione diretto con la propria Clientela, che rende possibile l'analisi, la definizione e l'implementazione di tutte le misure congiunte per la gestione della Crisi e per il recupero dei servizi e delle tecnologie di supporto quali, ad esempio, linee, apparati di sicurezza e connessioni.
In tal senso 3g Spa - quando possibile e richiesto - concorda coi propri clienti le modalità di reciproca collaborazione, quali: la definizione degli RTO e degli RPO, le connessioni da utilizzare in caso di disastro, i riferimenti da contattare per le comunicazioni generali, le azioni da compiere in caso di attivazione dell'infrastruttura tecnico-applicativa dal sito di Disaster Recovery, la pianificazione dei test.

4.5. Scenari di riferimento

L'ambito preso in considerazione può portare all'indisponibilità del sito relativo all'elaborazione dei dati. Nel caso di perdita di risorse umane si può ricorrere al servizio di quelle presenti nelle altre sedi operative della 3g.

Non si prendono invece in considerazione eventi che portino all'indisponibilità contemporanea di tutti i siti operativi. Viene considerata unicamente la continuità del processo di erogazione e non in generale dei processi di supporto quali, a titolo esemplificativo, Amministrazione, Gestione Risorse Umane.

4.6. Gestione dei contatti e delle comunicazioni

3g ha definito una adeguata struttura organizzativa al fine di gestire la procedura di escalation per la valutazione e l'eventuale Dichiarazione dello Stato di Crisi in azienda e la conseguente attivazione di soggetti di Business Continuity.
I soggetti coinvolti nel processo di gestione delle emergenze hanno il compito di gestire lo Stato di Emergenza e/o Crisi provvedendo alla gestione della comunicazione verso clienti e fornitori.
Il gruppo per la gestione del servizio risulta composto come di seguito indicato.

Riferimento persona fisica	Ruolo aziendale
A.Aracu	Presidente CDA
A. Aracu	Direzione Operativa
S. Aracu	DPO
F. Aracu	RSGI
F. Izzo	Amm. di rete

Modalità di comunicazione ai clienti
L'erogazione dei servizi in stato di Disaster Recovery deve essere comunicata ai clienti a mezzo telefono e/o fax o altra modalità attiva al momento del DR (es. Mail).

Modalità di comunicazione ai clienti
L'erogazione dei servizi in stato di Disaster Recovery deve essere comunicata ai clienti a mezzo telefono e/o fax o altra modalità attiva al momento del DR (es. Mail).

4.7. Simunlazione di disaster recovery

I suddetti scenari di crisi sono sottoposti a scenari di simulazione, in ambiente reale e/o virtuale, con frequenza non minore di una volta ogni anno.
Le registrazioni sono prodotte dal System Administrator e conservate per almeno 5 anni.

4.8. Revisione del Sistema di Gestione della Business Continuity

3g Spa effettua periodicamente, o a fronte di variazioni rilevanti, una revisione di tutto il Sistema di Gestione della Business Continuity (BCMS/BCP) per assicurare la sua rispondenza ed adeguatezza a fronte di cambiamenti normativi, organizzativi, strategici e legislativi.


3g
Human Technology

3G S.P.A.	DIREZIONE MONITORING E COMPLIANCE	DMP004PP	
POLITICHE E PROCEDURE DEL PERSONALE (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

IT SERVICE CONTINUITY PLAN

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIREZIONE MONITORING E COMPLIANCE	PRESIDENTE C.D.A.
4	**21/07/2023**	**AGGIORNAMENTO ISO**		

Contenuti

Sommario

Nome documento	IT Service Continuity Plan	Codifica	DMP004PP
Ufficio responsabile	Direzione Monitoring e Compliance	Data pubblicazione	31/07/2017
Indice revisione	Rev. 4	Data revisione	21/07/2023
Responsabile revisione	RSGI	Responsabile approvazione	Presidente C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017, ISO22301:2019, ISO/IEC27001:2013, ISO37001:2016, ISO45001:2018 SA8000:2014 UNI_PdR 125 2022 ISO 14064-2019 e ISO 50001-2018

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIREZIONE MONITORING E COMPLIANCE	PRESIDENTE C.D.A.
4	**21/07/2023**	**AGGIORNAMENTO ISO**		

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIREZIONE MONITORING E COMPLIANCE	PRESIDENTE C.D.A.
4	**21/07/2023**	**AGGIORNAMENTO ISO**		

IT SERVICE CONTINUITY PLAN

1. Introduzione

Il presente piano è stato sviluppato in conformità a quanto prescritto dalla norma di riferimento tenendo conto dei controlli e dei relativi aspetti dell'allegato A alla normativa UNI CEI ISO/IEC 27001 "Tecnologia delle informazioni. Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti". L'obiettivo è di contrastare le interruzioni delle attività relative al business, proteggerne i processi critici dagli effetti di malfunzionamenti significativi dei sistemi informativi o da disastri ed assicurare il loro tempestivo ripristino.
Questo documento delinea le procedure per la gestione della continuità operativa del servizio IT, con particolare riferimento alle piattaforme tecnologiche ed a quelle di rete. Questo documento riassume le procedure raccomandate.

2. Corpo della Procedura

2.1. Identificazione degli asset

Gli asset coinvolti nella gestione del presente piano sono elencati nel documento allegato

2.2. Descrizione del sistema

L'infrastruttura di Rete adottata da 3g è articolata come segue:

- Rete IP VPN MPLS a larga banda completamente ridondata che interconnetta tra loro le sedi 3g S.p.A. e la Server Farm di Milano Via Bernina 6 mediante circuito principale in Fibra Ottica in tecnologia SDH e backup a caldo, realizzato in diversità di tecnologia e di percorso, con circuito in rame in tecnologia CVP IMA.
- Dotazione per ciascuna sede di un accesso Internet a larga banda indipendente e ridondato, con circuito principale realizzato mediante Fibra Ottica in tecnologia SDH e backup in diversità di tecnologia e di percorso mediante circuito in rame in tecnologia SHDSL.
- Housing presso la Server Farm di Milano Bernina del sistema centralizzato per la gestione dei servizi fonia di tutte le sedi operative.

2.3. VPN MPLS

Per le proprie Unità Operative 3g S.p.A. ha un accesso VPN MPLS con le seguenti caratteristiche: Link Principale, con Tecnologia fibra SDH, PCR=MCR=100 Mbs e CPE: Cisco Router.
Link Backup, con Tecnologia CVP IMA, PCR=30 Mbs, MCR =10 Mbs;CPE: Cisco Router. Per la Server Farm, l'accesso VPN MPLS ha le seguenti caratteristiche:
Link Principale, Tecnologia: Gigabit Ethernet 100/1000 (connettore RJ45); PCR=MCR=200 Mbs; CPE: Cisco Router.
Link Backup, Tecnologia: Gigabit Ethernet 100/1000 (connettore RJ45); PCR=MCR= 200 Mbps; CPE: Cisco Router.
I router CPE sono configurati in HSRP per realizzare un meccanismo di backup a caldo che consenta di gestire eventuali fault in modo trasparente.
Sui router CPE sono implementati meccanismi di QoS che consentono in base a criteri di classificazione a livello di "trasporto" (layer 4 ISO/OSI) o superiore, di differenziare il traffico pregiato VoIP dal traffico dati best effort. In particolare al traffico VoIP sarà associata una classe di servizio a elevata priorità e bassa latenza con banda minima garantita.
I router Cisco utilizzati per l'accesso alla VPN MPLS delle sedi periferiche e della server farm consentono di scalare sino a 200 Mbps senza dover effettuare upgrade.
L'ampiezza di banda con cui sono dimensionati gli accessi alla VPN MPLS consente di garantire: per le sedi operative 3g S.p.A. una capacità pari a 300 canali VoIP bidirezionali e contemporanei in codifica

G729;
per la server farm una capacità pari a 720 canali VoIP bidirezionali e contemporanei in codifica G729.

2.4. Responsabilità

Responsabile SGSI si adopera affinché tutti i servizi IT siano attivati nel più breve tempo possibile nel caso in cui si verifichi un disastro.
Operatore: segnalare incidenti o potenziali incidenti (ipotesi di interruzioni di servizio),
CED: progettare soluzioni interne di configurazione hardware per gli applicativi, effettuare manutenzione alla struttura hw per applicativi, effettuare il monitoraggio di continuità e disponibilità dei servizi connessi alla struttura hw utilizzata per gli applicativi, registrare su modulistica di riferimento incidenti o potenziali incidenti (ipotesi di interruzioni di servizio) ai fini del miglioramento sistematico del presente documento, tenere sotto controllo interfaccia apposita.
AMM DI SISTEMA: progettare soluzioni interne delle reti dati, effettuare manutenzione alla rete interna, monitoraggio continuità e disponibilità dei servizi di connettività, segnalare incidenti o potenziali incidenti (ipotesi di interruzioni di servizio) ai fini del miglioramento sistematico del presente documento, tenere sotto controllo interfaccia apposita.

3. Attivazione del piano

3.1. Dichiarazione di disastro o incidente

Possono essere fornite le seguenti definizioni:

- Disastro: danno al sistema che dà luogo ad una interruzione di servizio

Incidente: un evento che non fa parte degli standard operativi del servizio e che causa o potrebbe causare una interruzione o riduzione della qualità del servizio

3.2. Valutazione di incidente

Tipologia di incidente:

Gravità:

4: impossibilità di erogazione del servizio
3: riduzione dei livelli di erogazione del servizio
2: i livelli di servizio sono garantiti a costi aggiuntivi per l'azienda
1: non influisce sui livelli di erogazione del servizio e sui costi preventivati

3.3. Procedura di ritorno alla normalità

Un incidente può essere considerato chiuso solo nel momento in cui il servizio è ritornato alla normalità operative.
Caso 1: incidenti di tipo operativo
L'incidente si ritiene chiuso nel momento in cui l'infrastruttura Hw/Sw preesistente sia stata completamente riparata o sostituita cioè conclusa l'attività prevista per il ritorno alla normalità descritta nelle tabelle precedenti.
Il tecnico incaricato dalla Direzione provvede a verificare l'effettivo ripristino, chiudendo la registrazione su modulo relativo. Lo stesso provvede a comunicare a chi ha segnalato l'incidente (via email) l'effettivo ritorno alla normalità del servizio.

3.4. Organizzazione del Team e Responsabilità

Segnalatore: comunica immediatamente l'incidente al CED CED: attivare le azioni di contenimento e ritorno alla normalità

4. Disaster recovery Plan

4.1. Scopo e campo di applicazione

Scopo del presente Piano di disaster recovery è definire l'insieme di misure tecnologiche atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business a fronte di gravi emergenze.

4.2. Disaster recovery Plan

Questa sezione del documento viene riesaminata almeno annualmente in occasione del riesame della Direzione o in occasione di richieste di modifica al piano di continuità a causa di incidenti (tecnico funzionali e/o sulla sicurezza IT) o migliorie richieste sul servizio.

4.3. Informazioni di supporto

4.3.1. Introduzione

Questo documento dettaglia le istruzioni e procedure che devono essere seguite dal personale tecnico di riferimento per ripristinare o continuare le operazioni dei sistemi, infrastrutture attrezzature mantenere la continuità del servizio ai livelli definiti o accordati con il business

4.3.2. Strategia di ripristino

I sistemi, infrastrutture, attrezzature devono essere sostituite da sistemi, infrastrutture o attrezzature alternativi in un tempo di ripristino approssimativo di **4 ore** (per le commesse gestite sui sistemi 3G).
Il sistema deve essere ripristinato all'ultimo punto di stabilità e di integrità dei dati conosciuto (attraverso il sistema di backup implementato), a cura del personale incaricato (responsabile manutenzione struttura e/o responsabile networking).

4.3.3. Linee guida

L'eventuale consultazione degli incidenti occorsi precedentemente è raggiungibile nell'archivio degli incident report.

In occasione di un potenziale o effettivo disastro rispettare i seguenti punti chiave:

- rimanere calmi ed evitare lunghe conversazioni
- informare il personale coinvolto delle modalità e tempistiche di escalation del ripristino (fornendo informativa sull'incidente occorso solo se strettamente necessario)
- tutte le attività devono essere gestite come un incidente (vedi incident report) con priorità 1 (critica)
- Tutte le attività e progresso delle stesse devono essere registrate su un incident report.

Per facilitare l'esecuzione delle attività chiave compilare la seguente check list:

Elemento	Obiettivo di completamento	Check completamento
Confermare che la comunicazione di disastro sia stata effettuata dal personale autorizzato	Segnalazione da Amministratore	
Identificare i problemi ed identificare il personale di gestione della crisi	Resp. Struttura e/o Networking aprono un TT	
Organizzare i supporti di backup, le informazioni critiche da trasferire nel locale di ripristino	Disponibilità dei supporti presso il locale di ripristino	
Avvisare gli utenti della possibilità di utilizzo del sistema di backup	Chiusura del TT	

4.3.4. Procedura di ripristino

Per gli incidenti conosciuti si faccia riferimento alle informazioni di seguito riportate:

a. Blackout

La continuità elettrica viene garantita tramite gruppi di continuità (UPS) e gruppi elettrogeni.

In caso di interruzione della fornitura di energia elettrica, stante le specifiche tutele contrattuali per tipologia di offerta, i sistemi UPS mantengono attivi tutti i sistemi.

- Server Farm di Milano in Via Bernina è un'infrastruttura in Tier IV con sistemi multipli, indipendenti e fisicamente separati sia per l'alimentazione e la a distribuzione dell'energia.
- Sede operativa Sulmona dotata di sistema automatico con UPS, che copre l'intera struttura, garantendo una continuità di esercizio di 15 minuti, e Gruppo Elettrogeno ad intervento automatico in pochi secondi dal rilevamento di interruzione dell'energia. Gruppo Elettrogeno in grado da garantire una continuità di erogazione dell'intera infrastruttura per circa 8 -10 ore a pieno carico di rifornimento.
- Altre sedi operative che mediante contratto di fornitura è garantito l'arrivo di gruppo elettrogeno secondo le modalità ed i tempi definiti nello specifico contratto. I sistemi UPS garantiscono un'autonomia di almeno 20 minuti a pieno carico ed i generatori a carburante diesel una produzione autonoma di energia con autosufficienza di almeno 30 ore a pieno carico tra i rifornimenti di carburante.

b. Attacco virale massiccio

Tutti i sistemi sono protetti da soluzioni antivirus costantemente aggiornate alle impronte virali eventualmente immesse nel circuito. La periodicità degli aggiornamenti è giornaliera.
L'eventuale presenza di virus è segnalata alla Control Room dal software di gestione centralizzata antivirus che lavora in compresenza di sistemi Firewall, IDS e IPS in grado di

identificare specifici pattern di comportamento e comunicazione, effettuando monitoraggio continuo delle comunicazioni da e verso l'esterno.
La navigazione su Internet è consentita solo a specifici profili di utenti ed esclusivamente attraverso proxy verso destinazioni approvate.
I sistemi di monitoraggio della Control Room vengono immediatamente allertati ad ogni evento critico ed allertano a loro volta su differenti canali i responsabili dei servizi (e-mail, sms).

Nel dettaglio, le soluzioni adottate sono le seguenti:

- Antivirus: Kaspersky Endpoint Security fo Business con aggiornamenti vari e in tempo reale
- Amministrazione centralizzata antivirus: Kaspersky Security Center Administration Server con aggiornamenti vari e in tempo reale
- IDS/IPS: Sistema UTM Unified Threart Management (gestione unificata delle minacce) con utilizzo di apparti FortiGate 200E
- Web Proxy: Squid e FortiGate 200E
- Firewall: FortiGate 200E.

c. Attacchi logici e di hacker

In ogni sede sono presenti i sistemi UTM costituiti da firewall, antivirus, IDS e IPS, che eseguono monitoraggio continuo delle attività che transitano sui sistemi e sulla rete.
Tutti i servizi accessibili dall'esterno sono protetti da sistemi firewall, WAF (Web Application Firewall) e mitigation anti-DDOS. I firewall applicano regole predefinite per consentire o inibire traffico e monitorano le comunicazioni verso i sistemi protetti per identificare e fermare eventuali attacchi o tentativi di intrusione.
Tali sistemi sono in grado di rilevare minacce di livello Network

Il WAF è un sistema in grado di rilevare minacce di livello Applicativo, monitorando le comunicazioni che coinvolgono i sistemi protetti ed identificando eventuali tentativi di attacco o intrusione.
Nello specifico, tali sistemi sono in grado di identificare Sql injection, attacchi cross -site XSS e vulnerabilità conosciute di software.
I sistemi sono protetti anche da due diversi sistemi di mitigation anti-DDOS, in grado di bloccare eventuali minacce di Distributed Denial of Service, il primo erogato in cloud da Cloudflare per mezzo di metodologie basate su reverse proxy, il secondo erogato da Fastweb per mezzo di sistemi Arbor Peakflow, che intervengono a livello network su protocollo BGP.
I sistemi di monitoraggio della Control Room vengono immediatamente allertati ad ogni evento critico ed allertano su differenti canali i responsabili dei servizi (e-mail, sms).

Nel dettaglio, le soluzioni adottate sono le seguenti:

- WAF: Cloudflare Business
- Mitigation anti-DDOS: Cloudflare Business, Fastweb FastKaleidos

d. Attacchi fisici (furto o danneggiamento)

Le soluzioni adottate sono le seguenti:

- presenza di sistemi di allarme

- controllo agli ingressi (reception e registro accessi)
- utilizzo di badge
- accesso controllato alle sale server

e. Down di sistema

La continuità dei servizi è garantita dalla completa ridondanza di tutti i sistemi.
Ogni sistema è dotato di doppia alimentazione elettrica ed è ridondato funzionalmente da un sistema identico, che si attiva in modalità automatica in caso di fault del componente principale. Dal punto di vista network, tutti i link sono ridondati su differente tecnologia, nel dettaglio: Datacenter Milano - doppio collegamento in fibra ottica, tutti gli apparati hardware in alta affidabilità:

- ogni server ridondato con doppia alimentazione e storage raid 1
- server ridondati con virtual ip, ogni server ha un server gemello in modalità attivo/passivo
- database: cluster di 2 nodi
- storage condiviso ridondato, raid 5
- n° 2 switch Cisco Catalyst 3750X con Etherchannel doppia alimentazione, ridondanza collegamenti con Lacp
- link Internet: n° 2 router Cisco 2821 (primario, backup), capacità link: 200 Mbps
- link MPLS: n° 2 router Cisco 2821 (primario, backup), capacità link: 200 Mbps

Altre sedi produttive - collegamento principale in fibra ottica, backup in rame (SHDSL) / tutti gli apparati hardware in alta affidabilità:

- ogni server ridondato con doppia alimentazione e storage raid 1
- server ridondati con virtual ip, ogni server ha un server gemello in modalità attivo/passivo
- database: cluster di 2 nodi
- storage condiviso ridondato, raid 5
- switch Cisco Catalyst 4506, Cisco Catalyst 3550. Spare disponibile in caso di fault.
- link Internet: n° 1 router Cisco (primario), n° 1 router Cisco (backup), capacità link fibra: 200 Mbps, backup SHDSL: 30 Mbps
- link MPLS: n° 1 router Cisco (primario), n° 1 router Cisco (backup), capacità link fibra: 100 Mbps, backup SHDSL: 30 Mbps

f. Rischio perdita dati a causa di fault dei sistemi di storage o di errore umano

Il mantenimento dei dati è garantito dalla presenza di hardware storage ridondato e da politiche di backup predefinite. Tutti i sistemi di storage sono in alta affidabilità, con ridondanza interna raid 1 o raid 5 e con sistema identico con modalità di failover attivo/passivo.
Risulta costantemente programmato il backup periodico giornaliero, settimanale e mensile di tutti i sistemi con seguente politica di retention:

- 30 set di backup giornalieri
- 8 set di backup settimanali
- 12 set di backup mensili

Nel caso il disastro non sia contemplato in tali casistiche le procedure verranno di volta in volta stabilite dal Responsabile Struttura e/o networking in accordo con la direzione aziendale e riportate nell'incident report.

5. Soggetti da informare

L'elenco dei soggetti da informare è il seguente: Responsabile Privacy, CED, Direzione, l'autorità garante (nei casi previsti dal Reg. UE 679/16), il Cliente.


3g
Human Technology

Nell'organizzazione e nella gestione delle attività operative si considera di fondamentale importanza porre particolare attenzione alla capacità di reazione alle emergenze, sia di tipo gestionale che di continuità operativa, che possano creare interruzioni che vanno assolutamente evitate.

La gestione ottimale del servizio parte sempre da un corretto dimensionamento delle risorse da dedicare alla erogazione dei servizi, tale da garantire una perfetta adesione dello staff predisposto alla curva di traffico ed il pieno rispetto degli SLA contrattuali e dei KPI qualitativi. 3g ha predisposto un piano digestione delle emergenze, che prevede una serie di misure da applicarsi in caso di eventi che possano compromettere la normale operatività come eventi che possono essere di natura tecnica, piuttosto che legati a variazioni dei volumi di lavorazione o ancora dipendenti da cause esterne.

Per gli aumenti di carico verranno utilizzati i seguenti ***strumenti***:

- ***Attivazione lavoro supplementare e straordinario*** – una percentuale degli operatori presenti in turno ha un contratto di tipo part time; questa caratteristica consente di avere a disposizione un bacino di ore utilizzabili come supplementari. Per gli operatori con contratto Full Time si procederà con gli straordinari. Tempo di adeguamento: immediato.
- ***Flessibilità multi-periodale*** **–** consente di distribuire l'orario lavorativo degli operatori non su una rigida suddivisione settimanale (ad es. 40 ore a settimana) ma in base ad una media, che viene calcolata su un periodo più lungo (un trimestre, un semestre, etc.): ricorrendo a tale misura è possibile pianificare una o più settimane con *un numero di ore maggiore rispetto a quelle standard*, che vengono poi "recuperate" in un periodo successivo, una volta cessato il picco.
- ***Attivazione piani di richiamo di operatori fuori turno*** – gli operatori fuori turno potranno essere richiamati in servizio in modo tale da incrementare la forza disponibile. Tempo di adeguamento: entro 12 ore.
- ***Inserimento di nuove risorse*** **–** tale misura risulta particolarmente efficace nel caso di eventi prevedibili, che abbiano un impatto a medio o lungo termine e comportino un aumento dei volumi significativo. In tali casi, infatti, è preferibile integrare il Gruppo di lavoro dedicato al servizio, con risorse che entrino a farne parte in maniera stabile e continuativa. Le risorse inserite ricalcano il percorso formativo del Gruppo di lavoro già operativo.

- ***Ricorso ad operatori condivisi*** – l'aumento di volumi di lavorazioni, anche non previsto e di notevole consistenza, può essere affrontato grazie al ricorso ad operatori impiegati anche in altri servizi e già perfettamente formati; tale misura garantisce un intervento estremamente rapido ed assicura il mantenimento della qualità erogata (ricorrendosi a risorse di comprovata esperienza).
- ***Team di Back Up*** – è un gruppo di lavoro "aggiuntivo", costituito da operatori dedicati ad altri servizi (analoghi per contenuto ed oggetto), che hanno partecipato alla formazione di start up ed in grado di essere immediatamente impiegati nella gestione dei servizi oggetto della Fornitura, al presentarsi di un picco, anche imprevisto/imprevedibile.
- ***Team di Emergenza*** – è un gruppo di operatori di comprovata esperienza e skill elevate, maturate in contesti simili per oggetto a quello della Fornitura, che viene chiamato a supporto del Gruppo di lavoro, in situazioni di emergenza ed in seguito ad un breve briefing formativo (della durata massima di un'ora), per gestire aumenti di carico di notevole consistenza e circoscritti ad una breve durata.

Le suddette attività vanno messe in campo, contestualizzandole, sia in caso di problematiche di routine che per incidenti che compromettano la continuità operativa di una singola attività, sede o aziendale.

Nel caso di incidente con compromissione della C.O. vanno subito contattati il responsabile del sistema di Continuità Operativa al numero 342.0591405 mail f.aracu@3gspa.net e il tecnico responsabile della Continuità Operativa al numero 342.0590753 mail f.izzo@3git.eu. In caso di mancata risposta allertare immediatamente il tecnico reperibile della sede coinvolta.

RCO

3G S.P.A.	AREA UFFICIO SISTEMI INFORMATICI	SI007PP	
POLITICHE SICUREZZA ACCESSI (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE PER L'ACCESSO AI SISTEMI INFORMATICI

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIRETTORE R.U.O. RESPONSABILE S.I. DIRETTORE COMPLIANCE	PRESIDENZA CDA
0	**01/02/2022**	-		

Contenuti

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIRETTORE R.U.O. RESPONSABILE S.I. DIRETTORE COMPLIANCE	PRESIDENZA CDA
0	**01/02/2022**	-		

GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE PER L'ACCESSO AI SISTEMI INFORMATICI

1 Obiettivi e finalità

Lo scopo della presente procedura è quello di definire un processo operativo, finalizzato alla razionalizzazione e alla standardizzazione dei flussi relativi all'attribuzione delle credenziali di autenticazione ed alla costituzione di un sistema di gestione delle stesse a livello aziendale.

Questa procedura fa parte del PIANO PRIVACY GENERALE 3G S.P.A. e si applica a tutte le sedi di 3g che impiegano lavoratori sulla commessa Fastweb.

🕮 **PIANO PRIVACY GENERALE 3G S.P.A.**

2 Responsabilità

Tutti gli Uffici sono interessati dal contenuto della presente procedura:

- L'Ufficio Risorse Umane è responsabile dell'attuazione della presente procedura.
- L'Ufficio Sistemi Informatici è responsabile della generazione, della modifica e della cancellazione degli accessi ai sistemi informatici.
- L'Ufficio Privacy è responsabile della conformità della presente procedura alla normativa GDPR.
- La Produzione è responsabile della supervisione e del controllo in merito al corretto utilizzo delle credenziali e dei dispositivi di autenticazione.

La presente procedura viene distribuita a tutte le funzioni coinvolte nel processo di attivazione, modifica e cancellazione delle credenziali informatiche.

RUP M001 PP/01 Dichiarazione procedura gestione credenziali

3 Applicativi/Software

- Sistema informatico aziendale.
- 3gHR.

4 Gestione delle credenziali informatiche e loro assegnazione

Ogniqualvolta un nuovo lavoratore (dipendente; somministrato; co.co.co.) o tirocinante (d'ora in avanti, solo "risorsa") viene assunto/avviato o cessato in 3g, l'Ufficio Risorse Umane provvede a gestire la relativa anagrafica nel sistema informatico aziendale tramite l'applicativo 3gHR tenuto conto delle seguenti istruzioni.

4.1. Stato del lavoratore nel sistema informatico aziendale

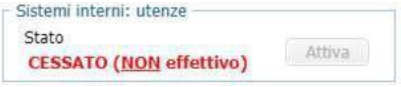
Per ogni risorsa presente nel sistema è visibile il suo stato rispetto ai sistemi interni ed un pulsante per richiedere le operazioni necessarie alla modifica di tale stato.
Di seguito un esempio per un lavoratore con utenze attive:

Gli stati possibili sono i seguenti:

- NUOVO – risorsa appena creata; operazione possibile: “Attiva”.
- ATTIVO – risorsa le cui utenze sono attive/abilitate; operazione possibile: “Cessa”.
- CESSATO – risorsa le cui utenze sono cessate/disabilitate; operazione possibile: “Attiva”.

In funzione dello stato, il pulsante presente nel riquadro consentirà l’operazione riportata nell’elenco precedente.

Se è stata richiesta un’operazione di attivazione o cessazione (come più avanti specificato), sarà riportato il nuovo stato, con la dicitura “non effettivo”, come nell’esempio (in cui è stata richiesta la cessazione):



In questo caso vuol dire che le procedure di attivazione o dismissione sono in corso; lo stato diverrà effettivo non appena saranno completate.

4.2. Operazioni sulle credenziali

Quando si digita pulsante Attiva/Cessa e si conferma la richiesta, una procedura automatica, che gira periodicamente, provvede ad inviare un’e-mail a chi di competenza (Ref. IT) per richiedere di avviare l’operazione richiesta su ciascuno dei sistemi interessati (i.e. 3gPortalCenter; Fastcenter; ContactCloud).

Nota per i tecnici informatici:
viene inviata un’e-mail – dall’account hr@3gspa.net – per ogni operazione per ogni sistema; l’e-mail elenca tutte le risorse individuate dopo la precedente esecuzione della procedura automatica, rapportandone username, cognome e nome;

- in caso di risorsa nuova, è specificata nell’e-mail la richiesta di creazione (oltre che di attivazione) delle utenze;
- l’attivazione e la dismissione per 3gPortalCenter, Fastcenter e ContactCloud sono automatiche;
- quando è stata completata l’operazione su un sistema per una determinata risorsa, al momento è necessario aggiornare lo stato della stessa come di seguito evidenziato; per il futuro vorrei integrare un link, da inserire nell’email delle operazioni, per ciascuna risorsa, in modo che, una volta cliccato, aggiorni lo stato dell’operazione (da verificare se attivo).

Quando vengono completate le operazioni su tutti i sistemi, una procedura automatica, che gira periodicamente, provvede ad aggiornare lo stato delle risorse interessate dal completamento, che sarà quindi visibile in 3gHR (la dicitura “non effettivo” scompare ed il pulsante viene abilitato).

4.3. Attivazione delle credenziali

Questa operazione, rispetto alla cessazione, ha una particolarità. Quando si digita il pulsante “Attiva”, 3gHR verifica l’esistenza di un contratto utile:

- se presente un contratto futuro (il più prossimo), o, in mancanza di questo, il contratto corrente, utilizza le sue informazioni per integrare l’attivazione con dei dati utili, come il fornitore, il ruolo della risorsa, il suo responsabile e, nel caso di lavoratore co.co.co., il contratto;
- diversamente, chiede di fornire tali informazioni (da inserire al posto dei puntini):

Queste informazioni risultano indispensabili in caso di creazione delle credenziali (ad esempio, per la corretta individuazione del ruolo da assegnare nel 3gPortalCenter) ed utili in caso di attivazione.

Nota per i tecnici informatici:
Queste informazioni vengono riportate nella e-mail, accanto ai dati dell’utente.

Di conseguenza, in maniera automatizzata, vengono generate le credenziali informatiche (“user/password”), la cui Password verrà modificata dall’operatore al primo accesso ai sistemi informatici. Tali credenziali vengono specificate e distribuite alla risorsa tramite il modulo denominato RUPM001PP/01 MODULO DI COMUNICAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE INFORMATICA. La distribuzione viene effettuata tramite il superiore diretto e copia del modulo viene archiviato digitalmente nel sistema informativo aziendale a cura dell’Ufficio Risorse Umane,

RUPM001PP/02 Modulo di comunicazione delle credenziali di autenticazione informatica

La risorsa abilitata si impegna a custodire e gestire con diligenza le credenziali assegnate e ad utilizzare gli strumenti di accesso ai sistemi per i soli fini lavorativi e nel rispetto di quanto previsto nel citato PIANO PRIVACY GENERALE 3G S.P.A.

4.4. Modifica account e cancellazione delle credenziali

Con adeguato anticipo (almeno 5 giorni lavorativi), il Coordinatore di Customer Care (Responsabile di Servizio) /diretto superiore comunica via e-mail all’Ufficio Risorse Umane e a Referenti BI eventuali modificazioni (i.e. cambio commessa, cessazione) rispetto all’utente attivato per consentire le necessarie modifiche nel sistema informativo aziendale.

In caso di cessazione del rapporto di lavoro/collaborazione/tirocinio per dimissioni/licenziamento/cessazione, l’Ufficio Risorse Umane comunica, nella data stessa dell’avvenuta cessazione, al Coordinatore di Customer Care (Responsabile di Servizio) /diretto superiore e a Responsabile BI tale evento. Ne consegue la chiusura del profilo della risorsa nel sistema informatico aziendale e la cancellazione automatica degli accessi.

Oltre alle credenziali informatiche, devono essere:

- cessate tutte le ulteriori credenziali di accesso ai sistemi dei Clienti secondo le procedure stabilite dagli stessi;
- disabilitato il badge aziendale personale;

- inibito l'accesso ai locali aziendali se non in qualità di ospite accompagnato da un responsabile aziendale.

4.5. Assenze di lunga durata

Ogni qualvolta una risorsa si assenta dal servizio per un lungo periodo (a titolo esemplificativo, per maternità, aspettativa, ecc.), l'Ufficio Risorse Umane comunica al Coordinatore di Customer Care (Responsabile di Servizio) /diretto superiore tale evento. Ne consegue la registrazione dell'uscita temporanea nel sistema informativo aziendale. In automatico, gli accessi vengono temporaneamente sospesi fino al rientro in servizio. Prima della ripresa dell'attività lavorativo, l'Ufficio Risorse Umane comunica nuovamente al Coordinatore di Customer Care (Responsabile di Servizio) /diretto superiore e a (???) tale evento con la data di rientro della risorsa. Ne consegue la riattivazione automatica degli accessi.

Ogni 3 mesi, al fine di verificare che tutte le utenze in uso siano valide e attive, il Coordinatore di Customer Care (Responsabile di Servizio) richiede l'estrazione di tutte le utenze esistenti con i relativi profili autorizzativi. Effettua un controllo e, se riscontra utenze inutilizzate o da cancellare/modificare, lo segnala all'Ufficio Sistemi Informatici e all'Ufficio Risorse umane.

5 Modulistica

- RUPM001PP/01 DICHIARAZIONE PROCEDURA GESTIONE CREDENZIALI
- RUPM001PP/02 MODULO DI COMUNICAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE INFORMATICA

6 Documentazione di riferimento e link

- PIANO PRIVACY GENERALE 3G S.P.A.
- http://172.16.0.31/3gportalcenter/.


3g
Human Technology

3G S.P.A.	AREA RISORSE UMANE E ORGANIZZAZIONE	RU002PP	
POLITICHE E PROCEDURE DEL PERSONALE (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

POLITICA AZIENDALE SUGLI STRUMENTI ED APPLICATIVI AZIENDALI

(AI SENSI DELL'ART. 4, COMMA 3 L. N. 300/1970 E DELL'ART. 23 D. LGS. N. 151/2015)

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIREZIONE RISORSE UMANE E ORGANIZZAZIONE	PRESIDENTE C.D.A.
0	01/08/2022	-		

Contenuti

Nome documento	Politica aziendale sugli strumenti ed applicativi aziendali	Codifica	RU002PP
Ufficio responsabile	Direzione Risorse Umane e Organizzazione	Data pubblicazione	01/08/2022
Indice revisione	Rev. 0	Data revisione	-
Responsabile revisione	Direttore Risorse Umane e Organizzazione	Responsabile approvazione	Presidente C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

Le informazioni contenute in questo documento sono di proprietà di **3g S.p.A.** (d'ora in avanti, solo "3g") e contrassegnate come "uso interno e riservatezza aziendale". Questo documento non può essere divulgato a nessuna parte al di fuori del pubblico a cui è destinato senza il permesso scritto di 3g. Questo documento non può essere riprodotto, né per fotocopia né per via elettronica senza il permesso scritto di 3g. Ogni destinatario di questo documento riconosce, mediante la conservazione e l'uso, la natura riservata del materiale contenuto nel presente documento e si impegna a impedire la distribuzione di questo documento, intenzionalmente o in altro modo, al di fuori del pubblico a cui è destinato.

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIREZIONE RISORSE UMANE E ORGANIZZAZIONE	PRESIDENTE C.D.A.
0	**01/08/2022**	**-**		

POLITICA AZIENDALE SUGLI STRUMENTI ED APPLICATIVI AZIENDALI

1 Premessa

3g S.p.A. (di seguito, per brevità, "Azienda" o "3g"), ai sensi del Regolamento Europeo n. 679 del 27 aprile 2016 (di seguito, per brevità, "GDPR") e sue successive modifiche e integrazioni, prevede la tutela delle persone e la protezione dei dati personali, partendo sempre da un approccio di "privacy by design" e "privacy by default", tramite la necessaria predisposizione di azioni volte a garantire sempre i principi di riservatezza, integrità e disponibilità secondo quanto sancito dal GDPR.

3g S.p.A. (di seguito, per brevità, "Azienda" o "3g") è da sempre attenta a garantire per i propri Clienti Committenti e per i propri lavoratori rigorose procedure di sicurezza nel trattamento e conservazione dei dati assicurando un elevato grado di riservatezza ed affidabilità attraverso le funzioni preposte e secondo gli standard di mercato.

2 Destinatari e finalità

La presente Politica aziendale è rivolta a tutti i dipendenti di 3g (di seguito, per brevità, "lavoratori"), ha la finalità di regolamentare il corretto utilizzo degli strumenti, degli applicativi, dei sistemi, delle reti e delle credenziali informatiche aziendali ed è stata redatta anche ai fini informativi previsti ai sensi dell'art. 4, Legge n. 300/1970, così come modificato dall'art. 23 D. Lgs. n. 151/2015, sul corretto utilizzo della strumentazione tecnologica aziendale affidata ai lavoratori per rendere la prestazione lavorativa, nonché sulle modalità di utilizzo degli strumenti ed applicativi aziendali, in modo che il predetto utilizzo risulti pienamente funzionale alla prestazione lavorativa.

Al riguardo si precisa che, in tutte le attività di trattamento effettuate tramite l'utilizzo di mezzi elettronici, l'Azienda osserverà le prescrizioni contenute nel Provvedimento Generale del 1° marzo 2007 emanato dal Garante per la Protezione dei Dati avente ad oggetto i trattamenti effettuati dai datori di lavoro riguardo all'uso, da parte dei lavoratori dipendenti, di strumenti informatici e telematici (posta elettronica e rete internet aziendale).

3 Regole generali

- I sistemi informatici, la rete aziendale, gli applicativi o software e i servizi forniti da 3g sono di proprietà dell'Azienda e devono essere utilizzati esclusivamente per finalità di lavoro.
- E' autorizzato esclusivamente l'utilizzo applicativi o software approvati da 3g, salva diversa autorizzazione aziendale.
- 3g garantisce la protezione della struttura e dei beni dell'organizzazione. L'Azienda, tuttavia, non è responsabile per la perdita, furto, danneggiamento e/o deterioramento degli oggetti personali che il lavoratore può portare e/o tenere sul posto di lavoro. Inoltre, si specifica che 3g non è responsabile di eventuali danni e/o furti che possono essere arrecati nelle aree esterne e/o nei parcheggi, nonché della loro regolamentazione o sicurezza.
- Il lavoratore è obbligato al corretto uso ed alla salvaguardia dei beni fisici e logici di proprietà dell'Azienda, ivi inclusi, a titolo esemplificativo ma non esaustivo, i sistemi informatici, stampanti e macchine multifunzione, gli strumenti aziendali assegnati individualmente, le informazioni e i dati, gli arredamenti ed il materiale a disposizione negli uffici e nelle sale operative. E' fatto divieto la disconnessione od il trasferimento di un qualunque dispositivo dalla sua locazione originale senza la necessaria autorizzazione da parte dall'Azienda.
- I beni e gli strumenti messi a disposizione dall'Azienda sono di proprietà 3g e, pertanto, il loro utilizzo è limitato esclusivamente allo svolgimento della prestazione lavorativa coerentemente con la funzione ricoperta. Pertanto, è fatto divieto di qualsiasi utilizzo difforme oppure per scopi illegali e/o di lucro,

commerciali o professionali diversi da quelli autorizzati dall'Azienda.

- L'accesso e l'utilizzo dei sistemi e della rete informatica, nonché tutti i dati ed informazioni dell'Azienda deve essere limitato esclusivamente alla prestazione lavorativa e, pertanto, è fatto divieto intraprendere attività illecite e/o illegali, lesive dei diritti e dell'immagine dell'Azienda, dei Clienti Committenti e di terze parti.
- E' dovere del lavoratore partecipare alle sessioni formative interne e/o esterne pianificate da 3g, ivi incluse le conferenze telefoniche, le visite mediche (sorveglianza sanitaria) e, più in generale, qualsiasi attività e/o evento inerente la prestazione lavorativa e/o col fine di migliorare le competenze professionali, cosi come l'integrità fisica e la sicurezza logica e fisica delle sedi operative e dei dati.

Le seguenti attività sono espressamente vietate:

- Disattivare o modificare i sistemi di monitoraggio e/o sicurezza (ad esempio software antivirus, applicativi criptografici, accessi tramite credenziali informatiche), su hardware e software di proprietà 3g, salvo diversamente stabilito dall'Ufficio Sistemi Informatici.
- Distruggere, modificare, disabilitare ovvero danneggiare in qualsiasi modo, ovvero fare un uso improprio della sistema informatico aziendale, PC/Laptop e apparecchiature associate, informazioni, dati, applicativi, software o documenti elettronici.
- Cercare di aumentare il livello di privilegi dell'utente nel sistema informatico aziendale, ottenere o tentare di ottenere informazioni senza essere autorizzato dall'Azienda.
- Utilizzare, alimentare (anche tramite rete elettrica aziendale) od installare dispositivi hardware esterni per uso personale: a titolo esemplificativo ma non esaustivo, smartphone, cellulari, agende elettroniche, unità USB, memorie flash, dispositivi MP3, Laptop, Tablet, masterizzatori, Hard drive, lettori CD/DVD/BLURAY, salvo diversa autorizzazione aziendale. Al riguardo, si precisa che è severamente vietato l'utilizzo di qualsiasi dispositivo hardware durante l'orario di lavoro (macchine fotografiche, radio, dispositivi MP3, lettori CD, Smartphone, etc.) e l'utilizzo di appunti cartacei per trattare dati personali nelle sale operative.
- Installare od utilizzare hardware o software non di proprietà o concessi in licenza ed approvati da 3g (a titolo esemplificativo ma non esaustivo, router, personal computer, altre apparecchiature) sulla rete 3g, salvo diversa autorizzazione aziendale.
- Rimuovere qualsiasi software installato dall'Azienda.
- Falsificazione o tentativo di falsificazione dei log di sistema.
- Monitorare in qualsiasi modo o cercare di entrare nei sistemi, algoritmi o in qualsiasi altro elemento di sicurezza che è attivo sui sistemi 3g.
- Utilizzare l'accesso ai sistemi 3g in modo fraudolento e come mezzo per accedere senza autorizzazione a determinate informazioni e/o risorse.
- Spacciarsi per qualcun altro (ad esempio, utilizzando le altrui credenziali informatiche).
- Utilizzare (anche in modalità vibracall/silenzioso) il telefono cellulare ad uso privato durante la permanenza nelle sale operative e negli uffici adibiti alla formazione. Pertanto, il telefono cellulare deve essere spento prima di accedere alle citate sale/uffici, salvo diversa autorizzazione aziendale.
- Fotografare, copiare, trasferire e/o salvare i dati delle carte di credito su hard disk/driver interni od esterni.
- Fotografare e/o rendere pubbliche immagini fotografiche e/o video acquisiti all'interno delle sedi 3g, salva diversa autorizzazione aziendale.

4 Sicurezza delle postazioni di lavoro

In qualità di Incaricato al trattamento dei dati, il lavoratore dovrà svolgere la propria attività lavorativa sempre nel rispetto del Regolamento Europeo n. 679 del 27 aprile 2016 (di seguito, per brevità, "GDPR") e della normativa in materia di privacy, pertanto è tenuto a:

- trattare i dati personali garantendo la massima riservatezza delle informazioni trattate;
- non stampare documenti aziendali contenenti dati personali o, laddove necessario, non lasciarli incustoditi;
- non gettare nella spazzatura documenti cartacei utilizzati nello svolgimento delle proprie attività lavorative contenenti dati personali se non dopo averli triturati (per maggiori dettagli, si rimanda alla **"Procedura aziendale in materia di privacy sulla distruzione dei documenti cartacei riportanti dati personali, giudiziari e particolari"**);
- bloccare il PC/Laptop in caso di assenza temporanea (utilizzando i tasti "Windows" + "L");
- adottare ogni cautela a protezione del dispositivo utilizzato, specialmente in caso di spostamenti;

In caso di allontanamento dalla postazione di lavoro durante o al termine dell'orario di lavoro, il lavoratore dovrà osservare le seguenti disposizioni, al fine di impedire l'accesso non autorizzato a terzi:

- bloccare il PC/Laptop in caso di assenza temporanea (utilizzando i tasti "Windows" + "L");
- evitare di lasciare incustodita la postazione di lavoro durante la sessione lavorativa;
- assicurarsi che il materiale contenente dati riservati sia riposto in un armadietto/cassetto chiuso.

In caso di trasferta/viaggio con un Laptop, Tablet od altro dispositivo di proprietà aziendale, il lavoratore dovrà:

- non lasciarlo in vista all'interno dell'autovettura incustodita;
- quando si viaggia in aereo, non imbarcare mai il Laptop nel bagaglio in stiva e fare attenzione alla possibilità di furto quando si passa attraverso i controlli di sicurezza negli aeroporti.
- tenerlo con sé in ogni momento, se possibile, o conservarlo in un contenitore chiuso.

E' responsabilità di ciascun lavoratore avere cura del Laptop/Tablet/Cellulare od altro strumento aziendale assegnato e notificare ogni possibile danno, perdita o furto dello stesso entro e non oltre un tempo massimo di 2 ore al proprio superiore e all'Ufficio Risorse Umane (risorseumane@3gspa.net). In caso di furto dello strumento aziendale è dovere del lavoratore procedere alla denuncia alle Autorità competenti, provvedendo ad inviare copia della stessa all'Ufficio Risorse Umane.

5 Sicurezza informatica

In qualità di Incaricato al trattamento dei dati, avendo necessariamente a che fare con dispositivi informatici nell'espletamento delle attività lavorative, il lavoratore dovrà sempre osservare il rispetto dei principi di integrità, riservatezza e disponibilità dei dati al fine di ridurre al minimo i rischi di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità oppure di distruzione o perdita dei dati stessi. A tale scopo ed in aggiunta alle regole generali più sopra riportate, il lavoratore deve:

- custodire con massima diligenza e non divulgare a terzi le credenziali di accesso;
- non memorizzare le credenziali di accesso sul dispositivo;
- non aprire, sia quando si lavora in rete sia quando lo strumento/dispositivo è utilizzato in locale, file sospetti e di dubbia provenienza;
- effettuare salvataggi e conservazione di dati solo ed esclusivamente su server aziendale, pertanto si ribadisce che è fatto assoluto divieto di effettuare salvataggi e conservazione di dati in locale (ad esempio, sull'hard disk del dispositivo);
- non introdurre o diffondere nella rete aziendale programmi illeciti (a titolo esemplificativo ma non esaustivo, virus, worm, spyware, etc.);
- non inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti;
- in caso di rilevazione di evento, incidente o segnalazione relativo alla sicurezza[1] (diverso dal "Data Breach" più avanti indicato), segnalarlo tempestivamente all'Ufficio Sistemi Informatici e al proprio diretto superiore, indicando in modo chiaro la natura del problema di sicurezza rilevato.

1 Qualsiasi fatto od evento che possa avere effetti sulla sicurezza personale od organizzativa.

- **nel caso in cui il software antivirus rilevi la presenza di un virus, sospendere ogni elaborazione in corso senza spegnere il PC/Laptop e segnalare tempestivamente l'evento all'Ufficio Sistemi Informatici e al proprio diretto superiore.**

6 Attestazione della presenza sul luogo di lavoro

- Ai fini del computo dell'orario di lavoro contrattualmente previsto e della corretta attestazione della presenza sul luogo di lavoro e a distanza laddove previsto (opzionando la relativa causale prima di effettuare la timbratura), il lavoratore dovrà effettuare la timbratura virtuale utilizzando l'applicativo 3G PORTAL CENTER direttamente nella propria postazione operativa di lavoro, secondo le seguenti modalità (salvo diversamente disposto):
  - ✓ Orario di lavoro con pausa pasto non retribuita (in via ordinaria, orario di lavoro a tempo pieno): una timbratura di entrata ad inizio orario di lavoro e a fine pausa pasto ed una timbratura di ad inizio pausa pasto, a fine orario di lavoro ed in caso di utilizzo di permesso (di qualsiasi natura). Nell'ipotesi che il termine del permesso non coincida con il termine dell'orario di lavoro, è prevista una timbratura in entrata a seguito di rientro al lavoro dal citato permesso.
  - ✓ Orario di lavoro senza pausa pasto non retribuita (in via ordinaria, orario di lavoro a tempo parziale): una timbratura di entrata ad inizio orario di lavoro ed una timbratura di uscita a fine orario di lavoro ed in caso di utilizzo di permesso (di qualsiasi natura). Nell'ipotesi che il termine del permesso non coincida con il termine dell'orario di lavoro, è prevista una timbratura in entrata a seguito di rientro al lavoro dal citato permesso.
- In caso di circostanze che impediscano un corretto uso del sistema di registrazione elettronico delle presenze, il lavoratore dovrà compilare l'apposito modulo di attestazione delle presenze disponibile sull'applicativo 3G PORTAL CENTER - che verrà autorizzato dal proprio responsabile gerarchico - segnalando gli orari di entrata/uscita fino al ripristino dell'applicativo stesso.
- Ogni richiesta di FERIE/ROL/EX FESTIVITA' od altro istituto previsto dal sistema dovrà essere preventivamente richiesta tramite l'applicativo 3G PORTAL CENTER.
- In caso di circostanze che impediscano un corretto uso dell'applicativo 3G PORTAL CENTER, Lei potrà richiedere FERIE/ROL/EX FESTIVITA' od altro istituto previsto dal sistema tramite preventivo invio via e-mail al proprio responsabile gerarchico con in copia l'Ufficio Risorse Umane (risorseumane@3gspa.net) fino al ripristino dell'applicativo.
- Si precisa che la reiterata dimenticanza/mancata timbratura delle presenze sarà considerata inadempienza disciplinarmente sanzionabile secondo le norme previste dalla normativa collettiva applicata al rapporto di lavoro.

7 Uso di Internet e della posta elettronica

- I messaggi di posta elettronica (di seguito, anche "e-mail"), una volta inviati, devono essere considerati come comunicazioni ufficiali e, pertanto, le informazioni contenute nelle e-mail devono essere attentamente selezionate. Tutti i messaggi di posta elettronica inviati da un dispositivo 3g sono di proprietà dell'Azienda.
- E-mail contenenti dati personali nel corpo del messaggio devono essere inseriti in file protetti da password ed inviati esclusivamente al soggetto autorizzato a conoscerne il contenuto (in tal caso la password per aprire il file dovrà essere inviata al citato soggetto tramite diverso canale quale, a titolo esemplificativo, SMS o WhatsApp).
- L'accesso a Internet è consentito esclusivamente per fini lavorativi e solo utilizzando il software approvato dall'Azienda.
- Aprire allegati di posta elettronica non attesi o ricevuti da un mittente sconosciuto/non attendibile è consentito esclusivamente dopo confronto con l'Ufficio Sistemi Informatici.
- Le e-mail devono essere sempre inviate utilizzando la firma elettronica aziendale standard definita da

3g, che comprende sia l'avviso legale che i dati personali del mittente.

Le seguenti attività sono espressamente vietate:

- Registrazione e pubblicazione su siti di social media (a titolo esemplificativo ma non esaustivo, Facebook, Instagram, LinkedIn, Twitter), newsgroup o forum usando il nome di 3g o l'indirizzo di posta elettronica aziendale, fatto salva diversa autorizzazione dell'Azienda.
- Invio di qualsiasi comunicazione e/o allegato per scopi diversi da quelli lavorativi, in grado di interferire con il processo di comunicazione verso terzi e/o di interrompere il normale funzionamento della rete aziendale.
- Falsificazione e/o alterazione dei messaggi di posta elettronica.
- Intercettazione, lettura, cancellazione, copia o modifica dei messaggi di posta elettronica o altre trasmissioni di rete inviati da terzi o destinati a terzi.
- Invio od inoltro di messaggi di posta elettronica a catena[2].
- Invio di messaggi o immagini, a titolo esemplificativo ma non esaustivo, di natura illegale, offensiva, diffamatoria, inappropriata, con contenuti discriminatori in materia di genere, età, sesso, diversa abilità, o materiale che promuove le molestie sessuali.
- Utilizzo della rete 3g, inclusa la connessione ad Internet, per giochi, lotterie, aste, nonché per il download di video, audio o di qualsiasi altro materiale estraneo all'attività lavorativa.
- La conservazione di e-mail contenenti dati personali nel corpo del messaggio o negli allegati oltre i 24 mesi, salvo il caso di loro anonimizzazione (cancellazione dei dati personali).

8 Proprietà industriale ed intellettuale

E' severamente proibito l'uso di software per PC/Laptop senza la relativa licenza, così come l'uso, la riproduzione, il trasferimento, la trasformazione o la diffusione di ogni tipo di opera od invenzione protetta oggetto di proprietà intellettuale od industriale di 3g, dei Clienti Committenti o di qualsiasi altra società.

9 Sistema di monitoraggio

- Al fine di assicurare il rispetto delle disposizioni e per motivi di sicurezza a tutela dell'Azienda (a titolo esemplificativo ma non esaustivo, necessità di effettuare verifiche sulla funzionalità e sulla sicurezza dei sistemi, constatazione di utilizzo indebito della posta elettronica e della rete Internet, presenza di casi di abusi da parte di singoli, presenza di indizi relativi alla fuga di informazioni confidenziali o riservate), 3g si riserva di monitorare e controllare in qualsiasi momento e senza preavviso tramite le funzioni designate come amministratori di sistema, l'utilizzo degli strumenti, dei suoi sistemi e della rete aziendale, a titolo esemplificativo:
  - ✓ PC/Laptop, cartelle condivise in rete, sulle quali vengono svolte attività regolari di controllo, amministrazione e back up che posso prevedere anche la rimozione di file o applicazioni ritenute pericolose per la sicurezza;
  - ✓ sessioni di Internet;
  - ✓ messaggi di posta elettronica inviati, ricevuti o composti usando l'account di posta elettronica aziendale;
  - ✓ tracciamento delle attività degli utenti, delle transazioni e degli eventi sulla sicurezza delle postazioni, server, applicazioni e di ogni altro dispositivo 3g o fisicamente installato in Azienda.
- Nel caso in cui si verificassero problemi di natura tecnica quali guasti o malfunzionamenti, l'Azienda

2 Messaggi intesi ad indurre chi li riceve a fare copie del testo del messaggio da diffondere su più soggetti diversi possibili. Metodi classici per indurre la diffusione sono storie emotivamente toccanti manipolate ad hoc, la possibilità di diventare ricchi secondo un modello piramidale, minacce di anatemi, di sventure, di violenza (anche fisica) o di morte qualora la catena venisse interrotta o le condizioni indicate nel messaggio non venissero accettate.

incaricherà dei tecnici specializzati al fine di rilevare e risolvere le cause dei guasti o dei malfunzionamenti che potranno determinare un'analisi approfondita dell'utilizzo del bene stesso.

- Nel caso di malfunzionamento di strumenti quali PC/Laptop, account di posta e rete internet, il personale incaricato potrà accedere ai dati riferibili a cookies, indirizzi IP, nome domini visitati, analisi della posta elettronica, allegati, download, account e qualunque file utile alla soluzione del problema, fermo restando la facoltà di accertare e segnalare eventuali abusi dei lavoratori che in tale sede vengano accertati.
- In ogni caso, l'Azienda utilizzerà impianti hardware e software quali firewall, antispam, antivirus e altri strumenti di controllo passivo con sistemi di filtraggio che consentano il blocco totale o parziale di determinati accessi a siti internet e che garantiscano la sicurezza di eventuali intrusioni illecite dall'esterno. Le strutture di controllo potrebbero raccogliere dati come indirizzi IP, cronologie, ping, cookie e altri dati di cui si effettuerà il trattamento in forma anonima. Suddetti dati saranno conservati per il periodo strettamente necessario e comunque non oltre tre mesi.
- I controlli come più sopra rappresentati sono effettuati al fine di verificare la sicurezza dei sistemi informatici aziendali e per garantirne la corretta manutenzione e saranno attuati nel pieno rispetto della privacy dei lavoratori e delle regole sul corretto trattamento dei dati personali che dovessero essere gestiti dall'Azienda.
- Il tutto verrà eventualmente fatto dall'Azienda, al ricorrere delle condizioni, nel rispetto dell'art. 4 della L. n. 300/70.

10 Istruzioni per la custodia delle credenziali informatiche

- Le password sono personali e segrete. Il lavoratore incaricato (di seguito, anche "Incaricato") da 3g al trattamento dei dati personali non deve in nessun caso fornire la propria User ID e/o password dei sistemi a nessuno, al fine di garantire l'integrità e la segretezza della/e password stessa/e.
- Se l'Incaricato sospetta che un'altra persona conosca la propria User ID e i dettagli della password, deve tempestivamente riportarlo al proprio superiore per l'assegnazione di una nuova User ID e/o password.
- L'Incaricato è responsabile della propria User ID e password assegnate per l'accesso ai sistemi. Tutte le operazioni effettuate dall'Incaricato nei sistemi con la propria User ID, verranno considerate come sotto la sua diretta responsabilità.
- Ogni Incaricato avrà la propria User ID esclusiva per accedere alle informazioni presenti nel sistema, pertanto, la User ID non può essere condivisa da più incaricati.
- In caso di recupero della password, dovrà esserne data immediata comunicazione all'Ufficio Sistemi Informatici, utilizzando l'indirizzo e-mail servicedesk@3git.eu, che provvederà alla reimpostazione temporanea della stessa (dopo il primo accesso dovrà essere obbligatoriamente modificata dall'utente).
- Le seguenti attività sono espressamente proibite:
  - ✓ condividere o fornire la propria User ID e/o password ad altri soggetti fisici e/o giuridici interni od esterni all'Azienda. La mancata osservanza di tale disposizione comporterà la considerazione dell'utente quale solo responsabile per azioni derivanti dall'individuo od entità non autorizzato all'uso della User ID;
  - ✓ lasciare User ID e/o password in evidenza presso la postazione di lavoro;
  - ✓ tentare di alterare o falsare i log del sistema;
  - ✓ tentare di decifrare codici, sistemi od algoritmi ed ogni altro elemento di sicurezza dei sistemi 3g;
  - ✓ utilizzare User ID e i privilegi ad essa associati in modo fraudolento e come mezzo di accesso ad informazioni o risorse per la quale non si è autorizzati.
- Nella scelta della password, questa deve essere composta da almeno otto caratteri e contenere lettere maiuscole, minuscole e caratteri speciali (a titolo esemplificativo, *,-,%) oppure, nel caso in cui il sistema non lo permetta, da un numero di caratteri pari al massimo consentito. La password non deve contenere riferimenti agevolmente riconducibili all'incaricato e deve essere modificata da quest'ultimo al

primo utilizzo e, successivamente, comunque almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la password deve essere modificata almeno ogni tre mesi.

- Al fine di assicurare la tutela dei dati personali e l'autotutela degli Incaricati, laddove applicabili dovranno essere poste in essere le seguenti disposizioni:
  - ✓ tutti i PC/Laptop in uso dovranno essere dotati di salvaschermo con parola chiave associata;
  - ✓ il salvaschermo dovrà essere impostato per entrare in funzione non oltre 120 secondi dopo l'ultima attività dell'incaricato;
  - ✓ la parola chiave associata al salvaschermo dovrà essere definita e modificata secondo le regole previste per tutte le parole chiave;
  - ✓ qualora gli strumenti in uso non consentissero l'uso di salvaschermo, sarà cura dell'incaricato, qualora sussista la necessità di allontanarsi, anche per brevi periodi, dalla propria postazione provvedere a disabilitarla utilizzando la MODALITÀ PAUSA.
- In caso di assenza pianificata è obbligatorio impostare come da istruzioni allegate il seguente messaggio di OUT OF OFFICE legato al proprio indirizzo e-mail aziendale:
  "Gent.mo/ma, sarò assente dal XXX al XXX. Se la richiesta è urgente è possibile contattare il seguente indirizzo e-mail XXX. In caso contrario, la richiesta sarà presa in carico il prima possibile al mio rientro. Cordiali Saluti, Nome Cognome".

11 Incidente di sicurezza (Data Breach)

Si rammenta che un uso non corretto (anche senza alcuna intenzione di dolo) delle strumenti/applicativi informatici aziendali sono spesso causa di violazioni di dati personali e incidenti informatici, come ad esempio nei casi di seguito elencati solo a mero titolo esplicativo ma non esaustivo:

- accesso non autorizzato;
- invio di e-mail contenenti dati personali e/o particolari a destinatario/i errato/i;
- virus o attacchi al sistema informatico o alla rete aziendale.

In caso di accertamento di una qualunque violazione di dati personali ("Data breach"), è fatto obbligo al lavoratore di applicare le disposizioni previste nella **Procedura di gestione "Data Breach"**.

12 Sicurezza fisica della sede di lavoro

- L'accesso alle sedi di lavoro dell'Azienda, nonché a determinate aree e/o uffici interni, è regolamentato tramite il badge assegnato individualmente.
- Ai fini della verifica della presenza in sede per motivi di, il lavoratore dovrà effettuare la timbratura fisica utilizzando l'apposito dispositivo presente all'ingresso delle sedi operative, secondo le seguenti modalità:
  - ✓ una timbratura di entrata all'ingresso nella sede operativa;
  - ✓ una timbratura di uscita all'uscita dalla sede operativa.
- L'accesso e la permanenza nei locali aziendali viene consentita esclusivamente durante l'orario di lavoro assegnato, previa identificazione tramite badge mostrato in maniera visibile.
- In caso di visita al di fuori dell'orario di lavoro, Il lavoratore dovrà registrarsi nell'apposito registro collocato presso la Reception/Ingresso ed esporre il proprio badge in maniera visibile.
- Si sottolinea che il badge con funzione di accesso è uno strumento aziendale attribuito individualmente, non è trasferibile e non può essere ceduto a terzi anche in via temporanea. Pertanto, è responsabilità di ciascun lavoratore averne cura e notificare ogni possibile danno, perdita o furto dello stesso entro e non oltre un tempo massimo di 2 ore al proprio superiore e all'Ufficio Risorse Umane (risorseumane@3gspa.net).
- In caso di interruzione del rapporto di lavoro con 3g, è obbligatoria la restituzione del badge, nonché di tutti gli strumenti aziendali eventualmente assegnati. La mancata restituzione comporta il relativo addebito del costo.

13 Inosservanza delle disposizioni aziendali

La presente Politica aziendale viene applicata in tutte le sedi di 3g e costituisce parte integrante del Regolamento aziendale e del codice disciplinare vigente in Azienda. Pertanto, la mancata osservanza, anche parziale, delle disposizioni ivi contenute sarà considerata inadempienza disciplinarmente sanzionabile in rapporto alla gravità del fatto e secondo le norme previste dalla legge e dalla normativa collettiva applicata al rapporto di lavoro.


3g
Human Technology

3G IT INNOVATION TECHNOLOGY S.R.L.	AREA UFFICIO SISTEMI INFORMATICI	SI002PP	
POLITICHE DI AGGIORNAMENTO PATCH (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

POLITICHE DI AGGIORNAMENTO PATCH

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	UFFICI/FUNZIONI IT	PRESIDENTE C.D.A.
2	12/04/2022	-		

3G IT INNOVATION TECHNOLOGY S.R.L.	AREA UFFICIO SISTEMI INFORMATICI	SI002PP	
POLITICHE DI AGGIORNAMENTO PATCH (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE INTERNA ESTERNA

Contenuti

Nome documento	Politiche di aggiornamento Patch	Codifica	SI002PP
Ufficio responsabile	Area Ufficio Sistemi Informatici	Data pubblicazione	10/12/2021
Indice revisione	Rev. 2	Data revisione	12/04/2022
Responsabile revisione	Izzo Fabio	Responsabile approvazione	C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	UFFICI/FUNZIONI IT	
2	**12/04/2022**	_		PRESIDENTE C.D.A.

POLITICHE DI AGGIORNAMENTO PATCH

1 Obiettivi e finalità

Applicare la patch di sicurezza sui sistemi informatici.

2 Responsabilità

- L'Ufficio Sistemi Informatici è responsabile del controllo e del rilascio delle Patch ai sistemi

3 Applicativi/Software

- Kaspersky Security Center
- Produttori software

4 Rilascio Vulnerabilità

A seguito dell'identificazione delle vulnerabilità vengono intraprese azioni di rilascio che posso avere modalità diverse, a seconda delle patch da installare.
Le vulnerabilità vengono rilevate secondo le modalità riportate nella policy di VA.

Il rilascio delle Vulnerabilità avviene con le seguenti modalità

- Sistema di rilascio delle patch integrato in Kaspersky Secutity Center
  - Prevalentemente utilizzato per postazioni Client
- Sistema di installazioni di pacchetti patch o aggiornamenti con installazione utilizzando il Kaspersky Secutity Center
- Utilizzo di aggiornamenti manuali su singoli Host seguendo le indicazioni del produttore

4.1. Rilascio delle Patch

Le patch di sicurezza vengono rilasciate prima su postazioni pilota, al fine di determinare eventuali impatti sull'operatività, e successivamente rilasciate per l'intera area di produzione. L'identificazione di patch più urgenti e di eventuali impatti sulla produzione vengono riportate all'interno del documento ed annotati i rilasci

- Event List vulnerabilità progressiva su anno

Nei casi in cui il rilascio non è applicabile in modo massivo, viene eseguito manualmente sul singolo dispositivo seguendo le istruzioni e modalità del singolo produttore di software

4.2. Controllo delle Patch applicate

La verifica dell'applicazione delle patch avviene tramite i report di VA che vengono prodotti mensilmente o quadrimestralmente

- Report VA kaspersky mensile
- Report VA Nessus Q1 - Q2 – Q3


3g
Human Technology

3G IT	AREA UFFICIO SISTEMI INFORMATICI	SI008PP	
POLITICHE DI GESTIONE ASSET (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

POLICY DI ASSET MANAGEMENT

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	RESPONSABILE IT	PRESIDENTE C.D.A.
3	26/06/2023	-		

Contenuti

Nome documento	Politica di Gestione Asset	Codifica	SI007PP
Ufficio responsabile	Area Ufficio Sistemi Informatici	Data pubblicazione	15/12/2021
Indice revisione	Rev. 3	Data revisione	26/06/2023
Responsabile revisione	Area IT	Responsabile approvazione	C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	RESPONSABILE IT	PRESIDENTE C.D.A.
3	**26/06/2023**	**-**		

POLICY DI GESTIONE ASSET

1 Obiettivi e finalità

Definire i requisiti per mappare e tracciare le risorse possedute durante il loro ciclo di vita. dall'acquisizione iniziale allo smaltimento finale.

2 Identificazione

La seguente politica si applica alle risorse 3g per garantire la corretta manutenzione, tracciamento, monitoraggio e gestione delle risorse.

3 Policy

La politica si applica agli asset fisici e virtuali, e dovrà essere mantenuto un inventario delle risorse al fine del tracciamento e monitoraggio. Tutte le attività significative saranno contabilizzate nell'inventario, gli articoli possono essere esclusi se comportano costi di acquisto bassi o presentano rischi minimi o nulli per le attività aziendali.
L'inventario dovrà contenere informazioni quali: descrizione del bene, area di appartenenza, e proprietario/responsabile. Il registro dovrà essere aggiornato ad ogni modifica e rivisto almeno annualmente.
Gli asset dismessi come guasti o obsoleti saranno trattati secondo apposita procedura.
A complemento sulla gestione degli asset, dovranno essere riportati I software installati e relative versione. La gestione potrà essere effettuata anche in modo separato e/o aggregato per gruppo di Asset,
in particolare nei casi in cui i dispositivi sono configurati con gli stessi software per aree specifiche. La verifica delle versioni potrà essere effettuata in coincidenza delle rilevazioni di vulnerabilità o a seguito di adeguamenti a specifiche richieste dei committenti. Gli aggiornamenti verranno annotati su apposito documento


3g
Human Technology

3G IT INNOVATION TECHNOLOGY S.R.L.	AREA UFFICIO SISTEMI INFORMATICI	SI003PP	
POLITICHE DI BACKUP (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

POLITICHE DI BACKUP

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	UFFICI/FUNZIONI IT	PRESIDENTE C.D.A.
3	12/04/2022	-		

Contenuti

Nome documento	Politiche di Backup	Codifica	SI003PP
Ufficio responsabile	Area Ufficio Sistemi Informatici	Data pubblicazione	10/12/2021
Indice revisione	Rev. 3	Data revisione	12/04/2022
Responsabile revisione	Izzo Fabio	Responsabile approvazione	C.D.A.

La presente politica è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO 9001:2015, ISO 14001:2018, ISO 18295:2017, ISO 22301:2019, ISO/IEC 27001:2013, ISO 37001:2016, ISO 45001:2018 e SA8000.

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	UFFICI/FUNZIONI IT	
3	**12/04/2022**	-		PRESIDENTE C.D.A.

POLITICHE DI BACKUP

1 Obiettivi e finalità

Sono state istituiti una serie di Backup su Server, Server DB e Server File Sharing al fine di preservare l'integrità e la conservazione delle informazioni in caso di guasti, attacchi informatici, vulnerabilità di sistema. La funzione è assicurare una copia di sicurezza delle informazioni.

2 Responsabilità

- L'Ufficio Sistemi Informatici è responsabile dei Backup

3 Applicativi/Software

- HBS 3 Hybrid Backup Sync
- Iperius Backup

4 Identificazione Server Backup

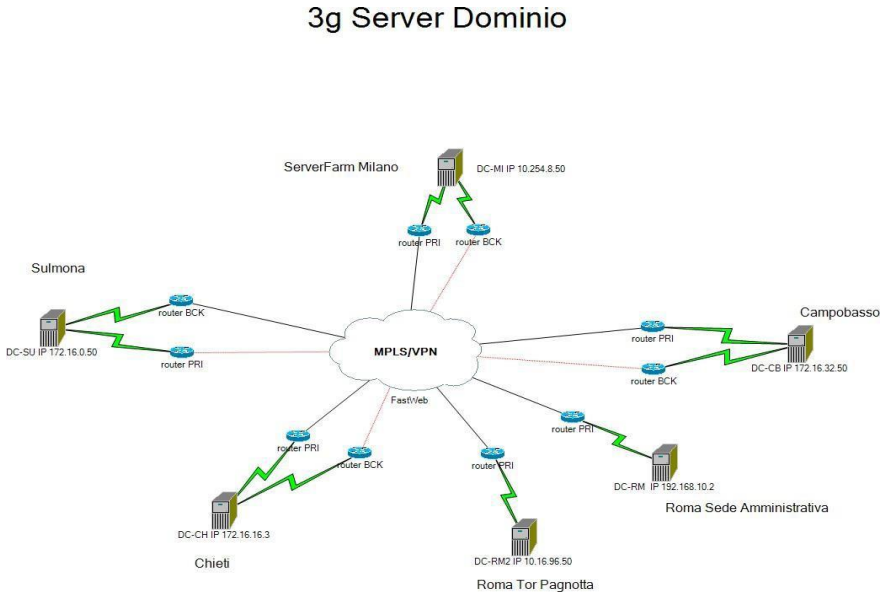
Sono stati individuati dispositivi per il Backup e soluzioni di continuità che non sono sottoposte a Backup

4.1. Server di Gestione Dominio

Tutte le strutture sono state dotate di Server di dominio con annesso server DNS.
E' stato configurato un dominio unico, denominato tregcc.local
Le strutture sono tutte collegate tra di loro, in caso di guasto o indisponibilità di un server su una struttura risponde il server collocato su un'altra sede.

La scelta di non effettuare backup dei server Controller di Dominio è nata dalla considerazione che tutti i server DC sono primari. In caso di guasto, il Server verrebbe ricreato dai cataloghi globali presenti su un altro dei server remoti.

Si riporta schema



4.2. Server di Backup

I Backup risiedono su dispositivi diversi

- NAS-Sulmona
- NAS-Roma
- NAS-Chieti
- NAS-Campobasso

4.3. Server file Sharing e conservazione documenti

All'interno dell'infrastruttura di rete 3g sono presenti NAS con aree di condivisione e conservazione di file.
I dispositivi sono i seguenti:

- NAS-Sulmona
- NAS-Roma
- NAS-Chieti
- NAS-Campobasso

4.4. Criticità e valutazione Rischio

Il backup non assicura in nessun caso una continuità di servizio, ma a secondo del server interessato, richiederà un intervento ed un ripristino con tempistiche diverse anche in funzione del tipo di Backup e del livello di compromissione.

Il ripristino di un Backup comporterà un fermo dei servizi interessati.

I tempi di fermo e ripristino sono valutati e riportati all'interno delle singole schede operative redatte per singolo Server.


3g
Human Technology

3G IT INNOVATION TECHNOLOGY S.R.L.	AREA UFFICIO SISTEMI INFORMATICI	SI005PP	
POLITICHE DI CYBERSECUTITY (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

POLITICHE DI CYBERSECURITY

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	RESPONSABILE IT	PRESIDENTE C.D.A.
3	23/06/2023	-		

Contenuti

Nome documento	Politiche di CyberSecurity	Codifica	SI005PP
Ufficio responsabile	Area Ufficio Sistemi Informatici	Data pubblicazione	10/12/2021
Indice revisione	Rev. 3	Data revisione	26/06/2023
Responsabile revisione	Izzo Fabio	Responsabile approvazione	C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	RESPONSABILE IT	PRESIDENTE C.D.A.
3	**23/06/2023**	-		

POLITICHE DI CYBERSECURITY

1 Obiettivi e finalità

Mitigare potenziali attacchi informatici.

2 Responsabilità

- L'Ufficio Sistemi Informatici è responsabile del controllo e delle soluzioni in essere

3 Applicativi/Software

- Kaspersky Security Center
- FortiMail
- FortiOS
- CloudFlare Business
- FastKaleidos

4 Politica

Al fine di implementare sistemi di sicurezza sono state implementate una serie sistemi di protezione ed azioni implementate o implementabili su tutta l'area aziendale.

Tutti i dispositivi Client devono essere dotati di sistema antivirus avanzato con funzioni:

- Protezione minacce da file
- Protezione minacce da Web
- Protezione minacce da Posta
- Firewall
- Protezione minacce di rete
- Rilevamento del comportamento anomalo del dispositivo per intercettazione Ransomware
- Blocco di malware su sfruttamento vulnerabilità software
- Prevenzione Intrusione Host
- Controllo dispositivi (Porte USB, dispositivi portatili, Smartphone, etc)

Tutti i sistemi aziendali devono essere protetti con sistemi di controllo e difesa avanzati di tipologia UTM con Firewall, Antivirus e IPS (Intrusion Prevention System). Il sistema deve permettere un monitoraggio attivo continuo delle attività che transitano sulla rete. I sistemi UTM devono essere aggiornati in tempo reale. Tutte le navigazione verso direttrici estere che non sono di interesse aziendale devono essere bloccate, a titolo di esempio ma non esaustivo (Est Europa, Asia, Medio Oriente, Africa, Sud America).Tutti i sistemi accessibili da esterno devono essere protetti da sistemi Firewall, WAF (Web Application Firewall) e mitigation anti-DDoS. Eventuali aggiornamenti delle regole sugli apparati di sicurezza dovranno essere annotati sul modulo predisposto. Nel caso, nel corso dell'anno solare, non venga effettuata nessun aggiornamento/revisione si dovrà procedere con almeno una revisione annuale delle regole.
Gli spazi di archiviazione (sia attivi che di backup) devono essere protetti da sistema di crittografia non deprecati.
La navigazione Web è consentita dalla LAN verso internet solo con protocolli sicuri (HTTPS). Le comunicazioni interne sia tra i siti che verso i committenti dovranno essere configurate in modalità sicura e tramite utilizzo di protocolli cifrati (esempio MPLS dedicate, VPN IPsec).

I sistemi informatici su rete pubblica (es.: rete Internet) sono configurati per eseguire la cifratura e la decifratura delle informazioni trasmesse. Per comunicazioni tra sistemi interni le chiavi crittografiche possono essere generate dai sistemi dedicati a tale operazione a cura dell'Area IT Aziendale. Le chiavi crittografiche utilizzate su sistemi che comunicano con terze parti, sono generate e gestite da Certification Authority esterne. Il processo di gestione del ciclo di vita delle chiavi crittografiche, a cura dell'Area IT.
L'uso di strumenti crittografici viene attuato nell'ambito del pieno rispetto della normativa vigente e in conformità con regolamenti ed accordi con terze parti. I sistemi utilizzati per la gestione di informazioni aziendali sono dislocati in locali sicuri, ad accesso controllato. La protezione è garantita da apposite contromisure per prevenire la violazione della riservatezza e della integrità sia fisica che logica, descritte rispettivamente nel Piano di Sicurezza Fisica e nella politica IT Gestione accessi.

L'intera insfrastruttura deve essere configurata con logica Hardening al fine di minimizzare gli impatti da possibili attacchi informatici, a titolo esemplificativo dovranno essere contemplate attività di (disabilitazione dei privilegi, disinstallazioni programmi non necessari, chiusura di porte, limitazioni a connessioni esterne, controllo della navigazione, controllo della posta elettronica, procedure d'accesso sicuro, gestione delle Patch e degli aggiornamenti).
L'utilizzo di account tecnici (generico) è consentito solo dove strettamente necessario, ed è controllato direttamente del responsabile alla sicurezza informatica che dovrà annotare ambito di utilizzo e personale autorizzate all'utilizzo.


3g
Human Technology

3G IT INNOVATION TECHNOLOGY S.R.L.	AREA UFFICIO SISTEMI INFORMATICI	SI004PP	
POLITICHE DI AGGIORNAMENTO PATCH (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 📖 INTERNA ▽ ESTERNA

POLICY DI GESTIONE ACCESSI

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	RESPONSABILE IT	PRESIDENTE C.D.A.
2	**26/06/2023**	**-**		

Contenuti

Nome documento	Policy di Gestione Accessi	Codifica	SI004PP
Ufficio responsabile	Area Ufficio Sistemi Informatici	Data pubblicazione	10/12/2021
Indice revisione	Rev. 2	Data revisione	26/06/2023
Responsabile revisione	Izzo Fabio	Responsabile approvazione	C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	RESPONSABILE IT	PRESIDENTE C.D.A.
2	**26/06/2023**	-		

POLICY DI GESTIONE ACCESSI

1 Obiettivi e finalità

Avere un controllo di gestione degli accessi in tutto l'ambiente tecnologico di 3g S.p.A.

2 Identificazione

Si applica a tutti i sistemi informativi utilizzati in tutta l'azienda sia gestiti centralmente che in modo distribuito. La policy si applica a tutti gli individui e le entità che accedono ai sistemi informativi ed ai dati dell'Azienda

3 Policy

La gestione degli accessi è il processo d'identificazione, tracciamento, controllo e gestione dei diritti di accesso degli utenti ai sistemi informativi.
Qualsiasi utente che richieda l'accesso a sistemi, applicazioni o dati deve avere la propria identità autenticata. Inoltre, l'accesso degli utenti dovrà essere ulteriormente limitato in base al principio dei privilegi minimi.
Il processo di creazione dell'account utente deve prevedere credenziali univoche per i nuovi utenti e la disabilitazione e/o la revoca dei privilegi di accesso di un utente al termine del rapporto di lavoro. Gli accessi degli utenti dovranno essere verificati con cadenza trimestrale, ed almeno annualmente la revisione dei ruoli di competenza per gli amministratori.
L'accesso privilegiato deve essere fornito agli utenti solo in base alle esigenze. Gli utenti con account utente privilegiati possono inoltre disporre di un account utente dell'organizzazione, che segue il principio del privilegio minimo, e devono utilizzare questo account utente dell'organizzazione per le funzioni lavorative quotidiane. Gli account utente con privilegi devono essere utilizzati solo quando il sistema o l'applicazione richiede privilegi elevati.
Tutti gli accessi remoti alla rete aziendale dovranno utilizzare un protocollo sicuro di crittografia di rete e, dove applicabile, utilizzare una soluzione di autenticazione a più fattori.
L'accesso logico e fisico a tutti gli elementi di sicurezza o funzionale è strettamente riservato al personale autorizzato.


3g
Human Technology

3G IT INNOVATION TECHNOLOGY S.R.L.	AREA UFFICIO SISTEMI INFORMATICI	SI006PP	
POLITICHE DI AGGIORNAMENTO PATCH (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 📖 INTERNA ▽ ESTERNA

POLICY DI LOG

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	AREA UFFICIO SISTEMI INFORMATICI	
1	**05/05/2022**	**-**		PRESIDENTE C.D.A.

Contenuti

Nome documento	Politica di Log	Codifica	SI004PP
Ufficio responsabile	Area Ufficio Sistemi Informatici	Data pubblicazione	10/12/2021
Indice revisione	Rev. 1	Data revisione	05/05/2022
Responsabile revisione	Izzo Fabio	Responsabile approvazione	C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	AREA UFFICIO SISTEMI INFORMATICI	
1	**05/05/2022**	**-**		PRESIDENTE C.D.A.

POLICY DI GESTIONE ACCESSI

1 Obiettivi e finalità

Registrazione degli accessi ai sistemi informatici da parte del personale e degli amministratori di sistemi. Registrazione degli accessi fisici delle sedi o di locali specifici.

2 Identificazione

Si applica a tutti i sistemi informativi utilizzati in tutta l'azienda sia gestiti centralmente che in modo distribuito. La politica si applica a tutti gli individui e le entità che accedono ai sistemi informativi ai dati dell'Azienda, agli accessi fisici delle sedi o locali aziendali.

3 Policy

Il metodo per effettuare il monitoraggio è costituito dalla raccolta ed analisi dei file di log.
La definizione ed il rilevamento degli eventi di sistema devono essere effettuati in funzione del valore dei dati, ed in modo tale da consentire la verifica dell'efficacia delle procedure di sicurezza. Ad esempio, ed ove possibile, dovrebbero essere rilevati:

- Autenticazione (login e logout)
- Accesso ai dati personali
- Modifica di funzioni da amministratore
- Connessioni di rete (ingresso e uscita)

Il log deve contenere (dove possibile):

- Data e ora
- Indirizzo IP o nome macchina
- Identità utente
- Descrizione dell'evento

I log raccolti devono essere raccolti tramite software concentratore e conservati su area riservata dove i file non sono modificabili. I dati sono conservati per un periodo minimo di 6 mesi. Eventuali eventi anomali, come orari di acceso in orari e/o giorni non lavorativi, tentativi di accesso con password errate, verranno segnalate in automatico tramite email al responsabile sicurezza informatica per tutte le verifiche del caso.
La stessa politica viene attuata anche per gli accessi fisici alle sedi o aree aziendali dotate di accesso controllato con badge. Gli accessi sono registrati e controllati all'occorrenza.


3g
Human Technology

3G IT INNOVATION TECHNOLOGY S.R.L.	AREA UFFICIO SISTEMI INFORMATICI	SI001PP	
POLITICHE DI VULNERABILITY ASSESSMENT (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

POLITICHE DI VULNERABILITY ASSESSMENT

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	UFFICI/FUNZIONI IT	PRESIDENTE C.D.A.
2	12/04/2022	-		

3G IT INNOVATION TECHNOLOGY S.R.L.	AREA UFFICIO SISTEMI INFORMATICI	SI001PP	
POLITICHE DI VULNERABILITY ASSESSMENT (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

Contenuti

Nome documento	Politiche di Vulnerability Assessment	Codifica	SI001PP
Ufficio responsabile	Area Ufficio Sistemi Informatici	Data pubblicazione	10/12/2021
Indice revisione	Rev. 2	Data revisione	12/04/2022
Responsabile revisione	Izzo Fabio	Responsabile approvazione	C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

Le informazioni contenute in questo documento sono di proprietà di **3g S.p.A.** (d'ora in avanti, solo "3g") e contrassegnate come "uso interno e riservatezza aziendale". Questo documento non può essere divulgato a nessuna parte al di fuori del pubblico a cui è destinato senza il permesso scritto di 3g. Questo documento non può essere riprodotto, né per fotocopia né per via elettronica senza il permesso scritto di 3g. Ogni destinatario di questo documento riconosce, mediante la conservazione e l'uso, la natura riservata del materiale contenuto nel presente documento e si impegna a impedire la distribuzione di questo documento, intenzionalmente o in altro modo, al di fuori del pubblico a cui è destinato.

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	UFFICI/FUNZIONI IT	PRESIDENTE C.D.A.
2	**12/04/2022**	**-**		

POLITICHE DI VULNERABILITY ASSESSMENT

1 Obiettivi e finalità

Monitorare ed applicare la patch di sicurezza sui sistemi informatici.

2 Responsabilità

- L'Ufficio Sistemi Informatici è responsabile del controllo e del rilascio delle Patch ai sistemi

3 Applicativi/Software

- Kaspersky Security Center
- Nessus

4 Identificazione Vulnerabilità

L'identificazione delle Vulnerabilità avviene attraverso utilizzo di strumenti e bollettini elencati di seguito:

- Sistema di monitoraggio VA integrato in Kaspersky Security Center
  - Dispositivi registrati all'interno delle strutture 3g
- Sistema di monitoraggio VA Nessus
  - Perimetro esterno
- Consultazione del CSIRT
  - https://csirt.gov.it/
- Consultazione di approfondimento CVE
  - https://www.cve.org/
  - Siti dei singoli produttori software ove necessario

4.1. Consultazione

Il sistema di monitoraggio VA integrato in Kaspersky viene consultato con cadenza settimanale, con cadenza mensile vengono estratti i report contenenti le Vulnerabilità non ancora applicate e con cadenza trimestrale viene redatta una relazione.
Il perimetro esterno delle strutture viene monitorato 3 volte l'anno nei seguenti periodi

- Marzo-Aprile
- Luglio-Agosto
- Novembre-Dicembre

I bollettini del CSIRT e relative consultazioni di approfondimento vengono consultate quotidianamente

4.2. Documenti a supporto

- Report VA kaspersky mensile
- Report VA Nessus Q1 - Q2 – Q3
- Relazione trimestrale sulla VA
- Event List vulnerabilità progressiva su anno

5 Documentazione di riferimento e link

Le patch vengono applicate utilizzando Kaspersky Security Center (ove applicabile). Dove non applicabili i rilasci degli aggiornamenti in modo massivo, vengono effettuati manualmente come indicato dal produttore del software.


3g
Human Technology

3G S.P.A.	AREA MONITORING E COMPLIANCE	DMP009PP	
POLITICHE E PROCEDURE DEL PERSONALE (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

PROCEDURA DI DISMISSIONE DEGLI ASSET INFORMATICI

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIREZIONE MONITORING E COMPLIANCE	PRESIDENTE C.D.A.
2	**07/02/2023**	**AGGIORNAMENTO ISO**		

Nome documento	PROCEDURA DI DISMISSIONE DEGLI ASSET INFORMATICI	Codifica	DMP009PP
Ufficio responsabile	Direzione Monitoring e Compliance	Data pubblicazione	04/06/2018
Indice revisione	Rev. 2	Data revisione	07/02/2023
Responsabile revisione	RSGI	Responsabile approvazione	Presidente CDA

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIREZIONE MONITORING E COMPLIANCE	
2	**07/02/2023**	**N/A**		PRESIDENTE C.D.A.

PROCEDURA DI DISMISSIONE DEGLI ASSET INFORMATICI (PC, DISPOSITIVI, SERVER) DI 3G S.P.A.

3g S.p.A. definisce la procedura per la dismissione degli asset non sono più utilizzabili da parte dei dipendenti o collaboratori o azienda.
Alla fine del ciclo utile, che corrisponde al momento in cui l'area IT definisce che il dispositivo non è più funzionale per l'attività prevista a causa di guasti irreparabili o per un funzionamento non più idoneo a causa del trascorrere di diversi anni, gli strumenti elettronici vengono dismessi.
Nel caso in cui ci siano dati personali all'interno del bene, questi vengono sottoposti all'attenzione dell'ufficio privacy che decide se trasferirli su un altro supporto o cancellarli definitivamente.
Nel caso in cui nel dispositivo non ci siano dati personali di cui 3g S.p.A. è Titolare o Responsabile, ai sensi del Regolamento UE 2016/679, si procede direttamente alla dismissione.
Nello specifico gli asset quali pc e server vengono formattati a livello idoneo dall'area IT e successivamente si procede alla distruzione materiale completa e definitiva.
I Responsabili di tale processo, cioè coloro che eseguiranno e assegneranno l'attività in base alla sede di riferimento, sono: Ermanno De Ritis, Carlo Lattanzio, , Mauro Vitale, Danilo Melaragni.
Essi si occuperanno di concludere la procedura fino all'ultima fase del processo. La procedura di dismissione avrà termine entro 3 giorni dal suo inizio.
Una volta terminata la procedura il Responsabile dovrà verificare che la stessa sia stata terminata
per per tutti gli apparati dismessi e che i pc, una volta distrutti gli HD, siano smaltiti secondo normativa vigente.

Colui che ha piena responsabilità di quanto accade durante tutto il processo è Fabio Izzo o sostituto da lui indicato in caso di sua lunga assenza.
Dal momento in cui il Responsabile avvia la procedura di dismissione entro 5 giorni bisognerà avvisare l'ufficio privacy di eventuali dati personali all'interno del dispositivo. L'ufficio privacy entro 5 giorni darà riscontro specificando se i dati presenti dovranno essere trasferiti in un'altra sezione o se possono essere cancellati e distrutti.
Una volta liberato il dispositivo dai dati personali, il Responsabile avvia la procedura di dismissione per la distruzione effettiva del bene che avverrà attraverso la distruzione di materiale dell'hard disk, e di ogni altra parte del dispositivo che si ritiene necessario distruggere, tramite un corpo contundente.
A conclusione della dismissione, sarà necessario compilare un documento di trasporto, a cura dell'amministrazione, intestato alla ditta o società che si occuperà dello smaltimento, specificando la descrizione e l'eventuale matricola dei beni, la quantità, la sede in cui erano ubicati e indicando come causale del trasporto "c/vendita fine ciclo vita", per poter aggiornare il registro dei beni ammortizzabili e implementare il registro Asset nella sezione dismissioni.
Per questo tipo di procedure si richiede al Responsabile che avvia il processo di dismissione di

informare tempestivamente il Consiglio di Amministrazione di 3g S.p.A. al seguente indirizzo: presidenzacda.3g@3gspa.net

Per qualsiasi informazione ulteriore riguardo la procedura è possibile contattare l'ufficio tecnico di riferimento in base alla sede di riferimento.

Per qualsiasi informazione ulteriore riguardo il trattamento dei dati personali all'interno dei dispositivi è possibile contattare il Comitato Privacy tecnico alla mail ufficioprivacy@3gspa.net o eventualmente il DPO all'indirizzo dpo@3gspa.net


3g
Human Technology

3G S.P.A.	AREA MONITORING E COMPLIANCE UFFICIO PRIVACY	DMP001PUP	
POLITICHE E PROCEDURE MONITORING E COMPLIANCE (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

PROCEDURA DI GESTIONE DATA BREACH

Contenuti

Nome documento	Procedura di Gestione Data Breach	Codifica	DMP001PP/01
Ufficio responsabile	Direzione Monitoring e Compliance	Data pubblicazione	28/05/2018
Indice revisione	Rev. 1	Data revisione	24/01/2022
Responsabile revisione	Ufficio Privacy	Responsabile approvazione	Presidente C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

REVISIONE MATRICE

REVISIONE	DATA	REVISIONE A CURA DI		APPROVATO DA
		SINTESI CAMBIAMENTI	DIREZIONE MONITORING E COMPLIANCE UFFICIO PRIVACY	PRESIDENTE C.D.A.
1	**24/01/2022**	**-**		

PROCEDURA DI GESTIONE DATA BREACH

1 Premessa

Per Data Breach si intende una violazione di sicurezza che comporta accidentalmente, o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. In tali casi la Legge impone al Titolare del trattamento, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, di notificare la violazione all'Autorità Garante per la protezione dei dati personali, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. E' altresì obbligatorio, in taluni casi, informare l'interessato senza ingiustificato motivo. A riguardo, una specifica procedura di data breach è essenziale per poter gestire l'evento, valutando la necessità o meno di notificare la violazione dei dati personali all'Autorità Garante e agli interessati qualora il rischio per gli stessi risulti elevato. Allo stesso tempo una policy condivisa è utile per prevenire ed abbassare il rischio che una violazione possa accadere, ma soprattutto per aiutare gli autorizzati a gestire la situazione nel caso in cui la violazione si verificasse.

2 Scopo

La procedura ha lo scopo di definire il flusso informativo per la gestione operativa di un eventuale data breach.

3 Campo di applicazione

La procedura si applica a tutte le attività di trattamento di dati personali riguardanti il personale, i clienti, i fornitori gestiti dai dipendenti/collaboratori su supporto cartaceo, informatico e tramite i dispositivi aziendali (PC fisso/PC portatile/cellulare).

4 Modalità di divulgazione

- Formazione;
- Invio a mezzo e-mail della procedura;
- Inserimento nel manuale operativo aziendale;
- Bacheche aziendali (virtuale e fisica);
- Consegna a ciascuna nuova risorsa in primo ingresso.

Definizione di **data breach**:

- una violazione di sicurezza (quindi un evento che incide sulla sicurezza dei dati personali che stiamo trattando);
- questa violazione, che sia accidentale o volontaria (quindi illecita), si individua come breach quando porta alla distruzione, alla perdita, alla modifica, alla divulgazione NON autorizzata o all'accesso (di persone non autorizzate) ai dati personali che stiamo trattando (quindi conservando oppure trasmettendo oppure elaborando, etc.).

Per gestire correttamente un data breach devo saper rispondere ad alcune domande:

- Come riconosco una potenziale violazione?
- A chi dovrò segnalare il data breach?
- Cosa devo scrivere?

Impariamo a riconoscere un data breach, di seguito alcune CASISTICHE DI VIOLAZIONE:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati al trattamento;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la modifica o la cancellazione di dati personali (sia accidentale che deliberata);

- l'impossibilità di accedere ai dati;
- la divulgazione non autorizzata dei dati personali.

Ora cerchiamo di identificare queste situazioni all'interno di alcuni possibili episodi che riguardano la vita lavorativa quotidiana e le misure che siamo tenuti a porre in essere in aggiunta alla segnalazione descritta nei punti successivi:

NB: ELENCO ESEMPLIFICATIVO NON ESAUSTIVO

CASISTICHE ESEMPLIFICATIVE	EFFETTO SUL DATO PERSONALE	MISURA DI MITIGAZIONE A CURA DI CHI RILEVA LA VIOLAZIONE
ESEMPIO N. 1 Invio di un' e-mail al destinatario sbagliato; attenzione l'e-mail potrebbe contenere dati personali o essere corredata da un allegato non criptato contenente dati personali	PERDITA DI RISERVATEZZA	Inviare immediatamente al destinatario errato il seguente messaggio: *"L'e-mail inviatale da questo indirizzo alle ore _____le è stata inoltrata per errore. La preghiamo pertanto di voler cancellare immediatamente il messaggio e tutti i suoi allegati, dandoci cortese riscontro di aver provveduto. La ringraziamo per la collaborazione, ci scusiamo per il disguido e Le ricordiamo che divulgare o trattare dati personali senza autorizzazione può costituire un illecito anche di tipo penale. Cordialità"* Attivare la procedura di segnalazione della violazione di cui ai successivi punto n. 5, 6, 7.
ESEMPIO N. 2 Distruzione del server (ad esempio a causa di incendio, allagamento, sbalzo di tensione, malfunzionamento)	PERDITA DI DISPONIBILITA', PERDITA DI INTEGRITA'	Attivare la procedura di segnalazione della violazione di cui ai successivi punto n. 5, 6, 7.
ESEMPIO N. 3 Perdita o furto del pc o del telefonino aziendale	PERDITA DI RISERVATEZZA, PERDITA DI DISPONIBILITA'	Attivare la procedura di segnalazione della violazione di cui ai successivi punto nn. 5, 6, 7.
ESEMPIO N. 4 Accesso illecito di un hacker sul proprio pc o apertura di un allegato	PERDITA DI RISERVATEZZA	Scollegare immediatamente il P.C. dalla rete web e spegnerlo senza riaccenderlo sino a nuova direttiva da parte della funzione Privacy\ICT

sospetto che potrebbe aver installato un virus nel sistema o avere avuto accesso alle informazioni contenute nel pc.		Attivare la procedura di segnalazione della violazione di cui ai successivi punto n. 5, 6, 7.
ESEMPIO N. 5 Cancellazione di file contenenti dati personali, senza copie di backup.	PERDITA DI DISPONIBILITA', PERDITA DI INTEGRITA'	Attivare la procedura di segnalazione della violazione di cui ai successivi punto n. 5, 6, 7.
ESEMPIO N. 6 Problema tecnico che non consente di accedere ai dati per un lungo periodo di tempo.	PERDITA DI DISPONIBILITA'	Attivare la procedura di segnalazione della violazione di cui ai successivi punto n. 5, 6, 7.
ESEMPIO N. 7 Mi accorgo che nel data base che utilizzo per sviluppare ad esempio i cedolini paga, o per effettuare gli stipendi, o per inviare UNILAV o altro ci sono degli errori nei dati che servono ad individuare con esattezza una o più persone. Mi accorgo di aver modificato per errore un file in cui sono conservati\elaborati dati personali e non ho una copia di backup	PERDITA DI INTEGRITA'-ESATTEZZA	Correggere immediatamente l'errore, avvisare eventualmente il destinatario cui fosse arrivato un documento non suo. Attivare la procedura di segnalazione della violazione di cui ai successivi punto n. 5, 6, 7.

5 Chi deve segnare il data breach e a chi deve segnalarlo

La segnalazione del data breach è un obbligo per **chiunque tratti i dati personali** per conto del Titolare del Trattamento.

Chi si rende conto della possibile violazione, è tenuto a informare immediatamente il superiore gerarchico, il quale a sua volta avvertirà l'Ufficio Privacy ed il DPO, nel caso in cui si verifichi uno degli eventi sopra descritti o si sia a conoscenza di eventi potenzialmente rischiosi.

L'Ufficio Privacy e il DPO si occuperanno di analizzare quanto accaduto.

6 Cosa bisogna scrivere

Al fine di garantire un efficace e tempestiva gestione del data breach è importante riconoscere il tipo di

violazione attraverso un'analisi dettagliata dell'accaduto, in modo da avere un quadro completo non solo delle cause, ma anche della tipologia di dati e dei soggetti coinvolti.

Occorre quindi relazionare l'accaduto inviando una prima SEGNALAZIONE informativa alla mail ufficioprivacy@3gspa.net descrivendo cosa è successo e dopo COMPILANDO il MODULO "data breach", qui in ALLEGATO e che potrai facilmente scaricare dalla intranet aziendale.

7 Come si deve inoltrare la segnalazione (a chi, entro quanto tempo?)

La segnalazione iniziale dovrà essere inviata immediatamente all'indirizzo mail ufficioprivacy@3gspa.net inserendo come oggetto "POSSIBILE DATA BREACH" e nel corpo del testo tutte le informazioni principali raccolte, entro e non oltre 15 minuti.

IL MODULO dovrà poi essere **inviato** , **senza ingiustificato ritardo e comunque non oltre 60 minuti dalla rilevazione della potenziale violazione,** a mezzo e-mail ad ufficioprivacy@3gspa.net con **oggetto: possibile data breach**.

Affinché la procedura di comunicazione sia efficace, è importante avere un riscontro effettivo che l'e-mail sia stata ricevuta.

La comunicazione avrà avuto certezza di ricezione solo in caso di risposta, da parte dell'ufficio privacy, che provvederà a riscontrare seguendo tale testo:

"La ringraziamo per la segnalazione che abbiamo provveduto a prendere in carico. La preghiamo di tenersi a disposizione ove fosse necessario un approfondimento rispetto a quanto da lei segnalato".

In assenza di riscontro, la comunicazione non è valida e deve essere effettuata nuovamente.

Bisogna poi assicurarsi che l'Ufficio Privacy abbia ricevuto tutte le informazioni utili alla ricostruzione della violazione per permettere una corretta valutazione e decidere insieme al DPO ed al Titolare del trattamento se notificare all'Autorità Garante/comunicare agli interessati l'evento.

NOTA BENE: LA VALUTAZIONE SULLA EFFETTIVA SUSSISTENZA DELLA VIOLAZIONE E DELLA SUA GRAVITA' NON SPETTA ALL'AUTORIZZATO, CHE È TENUTO SOLAMENTE A COMUNICARLA SECONDO LE MODALITÀ SOPRA DESCRITTE E AD APPLICARE LE MISURE DI MITIGAZIONE DI CUI AGLI ESEMPI N. 1 E 4 NELLE RELATIVE CASISTICHE.

8 Responsabilità

Qualsiasi violazione nell'osservanza della presente policy potrà essere considerata ai fini dell'adozione di provvedimenti disciplinari nei confronti del singolo dipendente; potrà essere giusta causa di recesso per le collaborazioni.

La responsabilità per la corretta applicazione della presente policy è dell'Ufficio Privacy e di tutti gli incaricati che a qualsiasi titolo gestiscono documenti del Titolare.

Nel caso l'autorizzato abbia qualsiasi dubbio afferente alle modalità in parola, deve rivolgersi all'Ufficio Privacy.

9 Modulistica

- DMP001PP/01-01 Modulo Segnalazione Evento Data Breach


3g
Human Technology

3G S.P.A.	DIREZIONE MONITORING E COMPLIANCE	DMP011PP	
POLITICHE E PROCEDURE DEL PERSONALE (SISTEMA DI GESTIONE INTEGRATO 3G S.P.A.)			REFERENZE 🕮 INTERNA ▽ ESTERNA

PROCEDURA PER IL MONITORAGGIO SICUREZZA

DEGLI ASSET

REVISIONE MATRICE

		REVISIONE A CURA DI	APPROVATO DA

1	16/03/2023	SINTESI CAMBIAMENTI **AGGIORNAMENTO ISO**	DIREZIONE MONITORING E COMPLIANCE	PRESIDENTE C.D.A.

Nome documento	Procedura per il monitoraggio sicurezza degli asset	Codifica	DMP011PP
Ufficio responsabile	Direzione Monitoring e Compliance	Data pubblicazione	14/11/2022
Indice revisione	Rev. 1	Data revisione	16/03/2023
Responsabile revisione	RSGI	Responsabile approvazione	Presidente C.D.A.

La presente procedura è parte del Sistema di Gestione Integrato 3g S.p.A. e si ispira ai principi aziendali e alle norme certificate ISO9001:2015, ISO14001:2015, ISO18295:2017,ISO22301:2019,ISO/IEC27001:2013,ISO37001:2016, ISO45001:2018 SA8000:2014 UNIPdR 125 2022 ISO 14064-2019 e ISO 50001-2018

Riservatezza/Avviso di sicurezza

Le informazioni contenute in questo documento sono di proprietà di **3g S.p.A.** (d'ora in avanti, solo "3g") e contrassegnate come "uso interno e riservatezza aziendale". Questo documento non può essere divulgato a nessuna parte al di fuori del pubblico a cui è destinato senza il permesso scritto di 3g. Questo documento non può essere riprodotto, né per fotocopia né per via elettronica senza il permesso scritto di 3g. Ogni destinatario di questo documento riconosce, mediante la conservazione e l'uso, la natura riservata del materiale contenuto nel presente documento e si impegna a impedire la distribuzione di questo documento, intenzionalmente o in altro modo, al di fuori del pubblico a cui è destinato.

REVISIONE MATRICE

REVISIONE		REVISIONE A CURA DI		APPROVATO DA
REVISIONE **1**	16/03/2023	SINTESI CAMBIAMENTI **N/A**	DIREZIONE MONITORING E COMPLIANCE	PRESIDENTE C.D.A.

MONITORAGGIO DELLA SICUREZZA DELL'ASSET

Il monitoraggio avviene nella maniera illustrata in tabella. Per ciascuna classe di "asset" l'RGSI e il responsabile Sistemi sono i responsabile di tutte le fasi di monitoraggio.

CLASSE DELL'ASSET	RESPONSABILE DELLA SICUREZZA DELL'ASSET	MONITORAGGIO E INDICATORI DI SICUREZZA	RESPONSABILE DEL MONITORAGGIO	PERIODICITÀ
Rete e comunicazioni	IT	Monitoraggio, misurazione e analisi dei log con alert inviati da dispositivi Firewall ed apparati di sicurezza: ▪ Attacchi volontari dall'esterno ▪ Attacchi volontari dall'interno ▪ Eventi per negligenza ▪ Eventi per incompetenza	RESP SISTEMI/RGSI	Continuo
Software	IT	Monitoraggio, misurazione e analisi dei risultati ottenuti dai test di VA sui perimetri interni ed esterni: ▪ Attacchi volontari dall'esterno ▪ Attacchi volontari dall'interno ▪ Eventi per negligenza ▪ Eventi per incompetenza	RESP SISTEMI/RGSI	Mensile
Dispositivi per l'elaborazione	IT	Monitoraggio, misurazione e analisi dei risultati ottenuti dai log con alert di dominio: ▪ Attacchi volontari dall'esterno ▪ Attacchi volontari dall'interno ▪ Eventi per negligenza ▪ Eventi per incompetenza	RESP SISTEMI/RGSI	Continuo

Controlli per la sicurezza

Le informazioni raccolte dal cliente e trattate successivamente dall'organizzazione sono informazioni critiche di livello A e come tali, conformemente al livello di rischio a cui sono esposte, sono protette dai controlli previsti dall'Annex A della norma ISO 27001:2017.
Viene controllata la conformità di

- Requisiti
- Progettazione
- Outsourcing
- Produzione
- Preservazione
- Controllo output non conformi

Procedure operative e responsabilità

Assicurare che le attività operative delle strutture di elaborazione delle informazioni siano corrette e sicure

Le attività di lavoro compiute al computer dagli autorizzati sono state individuate, descritte e attribuite secondo le indicazioni dell'organigramma.

Protezione dal malware

Assicurare che le informazioni e le strutture preposte alla loro elaborazione siano protette contro il malware

L'organizzazione ha provveduto all'installazione dell'anti malware grazie al quale provvede alla prevenzione della sicurezza delle informazioni gestite.

Le altre azioni adottate e specificate nelle procedure di verifica sono le seguenti:

- È installato un adeguato sistema di difesa perimetrale (firewall)
- Sono eseguiti backup periodici assicurandosi che la copia dei dati salvati venga conservata al sicuro
- Vengono aggiornati i sistemi operativi
- Il sistema di rete è dotato di automatizzazione degli aggiornamenti
- Viene verificato che l'anti malware sia sempre aggiornato
- Si proibisce di aprire mail sospette
- Si proibisce di cliccare su aggiornamenti o call to action poco attendibili


3g
Human Technology