					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P32S					Titolo del documento: **Politica di continuità operativa e ripristino di emergenza**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento a norme e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 6.1, 6.3, 8	
ISO/IEC 27002:2022	Controlli 5.29, 5	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
GDPR UE	Articoli 32, 33	
NIS2 UE	Articolo 21(2)(f)	
DORA UE	Articolo 10	
COBIT 2019	DSS	

1. Finalità

1.1 La presente politica garantisce che l'organizzazione sia in grado di mantenere la continuità delle operazioni aziendali e ripristinare i servizi IT essenziali durante e dopo eventi di interruzione quali interruzioni dell'alimentazione elettrica, attacchi informatici, infezioni da ransomware o guasti dei sistemi.

1.2 Essa definisce un quadro di riferimento chiaro per la pianificazione della continuità operativa e del ripristino di emergenza (BC/DR), adattato alle PMI prive di team IT dedicati.

1.3 La presente politica supporta l'organizzazione nel soddisfacimento dei requisiti obbligatori previsti da ISO/IEC 27001:2022, GDPR, NIS2, DORA e COBIT 2019, rafforzando al contempo la resilienza operativa e la fiducia dei clienti.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutti i sistemi e i servizi critici per l'operatività aziendale (ad es. posta elettronica, archiviazione cloud, piattaforme di fatturazione, registrazioni dei clienti)

2.1.2 Tutti i dipendenti e i fornitori esterni di servizi IT responsabili della preparazione e dell'esecuzione del BC/DR

2.1.3 Tutte le tipologie di interruzione, inclusi incidenti informatici, guasti hardware, perdita di alimentazione, allagamenti e inaccessibilità degli uffici

2.2 Essa comprende:

2.2.1 la gestione dei backup

2.2.2 la pianificazione della continuità operativa (BCP)

2.2.3 le operazioni di ripristino di emergenza

2.2.4 la formazione del personale e i test

2.2.5 le procedure di risposta legale e regolatoria

3. Obiettivi

3.1 Proteggere la capacità dell'organizzazione di erogare servizi chiave nonostante interruzioni non pianificate.

3.2 Garantire il tempestivo ripristino di sistemi e dati in conformità agli obiettivi di tempo di ripristino (RTO) predefiniti.

3.3 Consentire a tutto il personale di seguire le procedure di continuità durante le crisi, con il minimo impatto sull'operatività.

3.4 Mantenere la conformità normativa in materia di protezione dei dati e resilienza operativa, incluso l'articolo 32 del GDPR e l'articolo 21 della NIS2.

3.5 Stabilire una strategia di continuità e ripristino pratica, verificabile e adeguata alle PMI.

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 È il titolare del processo BC/DR e della presente politica

4.1.2 Approva il Business Continuity Plan (BCP)

4.1.3 Coordina la risposta agli incidenti e la comunicazione interna durante le interruzioni

4.1.4 Effettua le notifiche regolatorie richieste (ad es. notifiche di violazione dei dati personali ai sensi del GDPR)

4.2 Fornitore IT / Amministratore di sistema

4.2.1 Mantiene ed esegue i test dei backup

4.2.2 Esegue le procedure di ripristino di emergenza quando attivate

4.2.3 Documenta tutte le azioni di ripristino e gli eventi di ripristino dei sistemi

4.2.4 Segnala immediatamente al GM gli incidenti IT critici

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1 Riesame annuale della politica e del piano

9.1.1 Il Direttore generale (GM) deve garantire che la presente politica e il relativo Business Continuity Plan (BCP) siano formalmente riesaminati almeno una volta all'anno.

9.1.2 Il riesame deve includere:

9.1.2.1 valutazione di rischi nuovi o emergenti

9.1.2.2 riconvalida di RTO/RPO

9.1.2.3 verifica delle informazioni su fornitori e contatti

9.1.2.4 allineamento alle modifiche dei sistemi IT, degli obblighi legali o delle operazioni

9.2 Aggiornamenti basati su eventi attivanti

9.2.1 La presente politica deve essere aggiornata anche in risposta a:

9.2.1.1 incidenti rilevanti o interruzioni, soprattutto se gli obiettivi non sono stati raggiunti

9.2.1.2 nuovi obblighi legali o regolatori (ad es. modifiche a DORA)

9.2.1.3 modifiche a sistemi critici, piattaforme cloud o personale

9.2.1.4 risultanze dei test annuali BCP/DR

9.3 Processo di controllo delle modifiche

9.3.1 Tutte le modifiche devono essere approvate dal GM

9.3.2 Deve essere mantenuta una cronologia delle versioni, inclusa la data, la descrizione della modifica e il soggetto approvante

9.3.3 La politica aggiornata deve essere nuovamente distribuita a tutto il personale interessato, incluso il fornitore IT e i responsabili di funzione

9.4 Documentazione delle lezioni apprese

9.4.1 Dopo i test o le interruzioni reali, le lezioni apprese documentate devono confluire negli aggiornamenti successivi

9.4.2 Tali riesami devono includere anche valutazioni delle prestazioni dei fornitori e verifiche di adeguatezza della risposta

10. Politiche correlate e collegamenti

10.1 La presente politica è strettamente integrata con le seguenti politiche SME:

10.1.1 P1S – Politica per la sicurezza delle informazioni: definisce gli obiettivi di sicurezza di alto livello che le pratiche di continuità e ripristino devono supportare.

10.1.2 P4S – Politica di controllo degli accessi: consente la revoca degli accessi o il ripristino di emergenza degli accessi utente durante scenari di interruzione dell'attività.

10.1.3 P6S – Politica di gestione del rischio: costituisce il fondamento per identificare, valutare e dare priorità ai rischi connessi alla continuità.

10.1.4 P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: garantisce che i dipendenti siano preparati ad agire durante le interruzioni e comprendano il BCP.

10.1.5 P15S – Politica di backup e ripristino: fornisce procedure tecniche specifiche per tutelare la disponibilità dei dati e il recupero.

10.1.6 P17S – Politica di protezione dei dati e privacy: garantisce che la pianificazione della continuità rispetti la tutela dei dati personali e il GDPR durante e dopo gli incidenti.

10.1.7 P22S – Politica di registrazione e monitoraggio: supporta il rilevamento degli eventi che possono attivare i processi BC/DR e fornisce tracce di audit forensi dopo l'interruzione.

10.1.8 P30S – Politica di risposta agli incidenti (P30): precede direttamente l'attivazione del processo di ripristino in caso di incidenti informatici o operativi.

10.1.9 P31S – Politica di raccolta delle evidenze e forense: garantisce che le evidenze digitali siano acquisite durante scenari di continuità per esigenze di conformità, assicurative o investigative.

10.2 Tali politiche costituiscono un quadro coerente, pronto per gli audit, a supporto della resilienza, dell'accountability e della continuità dei controlli in tutte le operazioni delle PMI.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001:

11.1.1 Clausola 6.1 – Richiede pianificazione e trattamento basati sul rischio, inclusi continuità operativa e ripristino.

11.1.2 Clausola 6.3 – Sottolinea il miglioramento continuo a seguito delle interruzioni.

11.1.3 Clausola 8.1 – Impone controlli operativi, che comprendono misure di continuità documentate.

11.2 ISO/IEC 27002:

11.2.1 Controllo 5.29 – Richiede l'istituzione e il mantenimento di misure di continuità operativa.

11.2.2 Controllo 5.30 – Richiede il test e il riesame di tali misure.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – Definisce i requisiti per la pianificazione di contingenza.

11.3.2 CP-4 – Impone la formazione del personale dell'organizzazione in materia di contingenza.

11.3.3 CP-6 – Copre i requisiti relativi al sito alternativo di archiviazione.

11.3.4 CP-7 – Disciplina i requisiti relativi al sito alternativo di elaborazione.

11.4 GDPR UE:

11.4.1 Articolo 32 – Richiede misure volte a garantire la continua disponibilità e resilienza dei sistemi e dei servizi di trattamento.

11.4.2 Articolo 33 – Attiva gli obblighi di notifica della violazione dei dati personali nei casi in cui il guasto della continuità comporti la compromissione di dati personali.

11.5 Direttiva NIS2 UE (2022/2555):

11.5.1 Articolo 21(2)(f) – Richiede capacità di pianificazione della continuità operativa e di gestione delle crisi come condizione di preparazione al rischio informatico.

11.6 Regolamento DORA UE (2022/2554):

11.6.1 Articolo 10 – Impone l'attuazione di test di resilienza operativa digitale e capacità di ripristino, in particolare per le PMI del settore finanziario.

11.7 COBIT 2019:

11.7.1 DSS04 – Gestire la continuità: fornisce indicazioni di governance aziendale per mantenere e convalidare la resilienza operativa, inclusi titolarità, test, integrazione dei fornitori e riesami successivi all'evento.