					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P32					Titolo del documento: **Politica di continuità operativa e disaster recovery**							
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 standard e normative applicabili

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	
ISO/IEC 27002:2022	Controlli 5.29, 5.30	
NIST SP 800-53 Rev.5	Da CP-1 a CP-11	
NIST SP 800-34 Rev.1	Pianificazione della continuità operativa	Quadro di riferimento
ISO 22301:2019		Requisiti del sistema di gestione della continuità operativa
GDPR UE	Articolo 32	
Direttiva UE NIS2	Articolo 21(2)(f)	
Regolamento UE DORA	Articolo 10	
COBIT 2019	DSS04	

1. Finalità

1.1. La presente politica definisce i controlli obbligatori e le responsabilità necessari a garantire la capacità dell'organizzazione di mantenere o ripristinare le operazioni aziendali critiche e i servizi ICT di supporto durante e dopo un incidente dirompente.

1.2. La politica ha l'obiettivo di tutelare la vita, la stabilità operativa, gli obblighi di legge, gli impegni verso i clienti e la reputazione dell'organizzazione, integrando la resilienza attraverso una pianificazione proattiva e capacità di ripristino validate.

1.3. La presente politica costituisce il fondamento del quadro di riferimento dell'organizzazione per la gestione della continuità operativa (BCM) e il disaster recovery (DR), garantendo la conformità ai requisiti normativi, contrattuali e di settore applicabili.

2. Ambito di applicazione

2.1. La presente politica si applica a tutte le unità organizzative, ai sistemi informativi, ai processi aziendali, al personale e ai servizi erogati da terze parti classificati come critici o essenziali sulla base dei risultati della Business Impact Analysis (BIA).

2.2. La politica copre:

2.2.1. Interruzioni di origine naturale o antropica, inclusi attacchi informatici, guasti infrastrutturali, indisponibilità del data center, pandemie e interruzioni dei servizi dei fornitori.

2.2.2. Pianificazione, test e miglioramento continuo dei Piani di continuità operativa (BCP) e dei Piani di disaster recovery (DRP).

2.2.3. Ruoli e responsabilità per la risposta alle emergenze, il coordinamento del ripristino e l'escalation degli incidenti.

2.3. Tutto il personale con responsabilità in materia di continuità operativa o ripristino, inclusi IT, titolari di processo, responsabili della gestione delle crisi e fornitori, è soggetto alle disposizioni della presente politica.

3. Obiettivi

3.1. Garantire la continuità delle operazioni e dei servizi aziendali mediante procedure predefinite e testate, riducendo al minimo l'impatto operativo, reputazionale e legale.

3.2. Ripristinare i servizi ICT entro i Recovery Time Objective (RTO) e i Recovery Point Objective (RPO) definiti, in coerenza con i livelli di tolleranza al rischio aziendale.

3.3. Assegnare la responsabilità della pianificazione, dell'esecuzione e della governance della continuità operativa e del disaster recovery all'interno dell'intera organizzazione.

3.4. Garantire che le capacità di continuità siano sottoposte regolarmente a test, mantenute e migliorate sulla base di scenari realistici e dei rilievi di audit.

3.5. Soddisfare gli obblighi di conformità previsti da ISO, NIST, GDPR, DORA e NIS2, a supporto della dovuta diligenza in materia di resilienza operativa e disponibilità.

4. Ruoli e responsabilità

4.1. Direzione aziendale

4.1.1. Approva la Politica di continuità operativa e disaster recovery e ne assicura l'allineamento strategico.

4.1.2. Assegna budget e risorse a supporto della continuità operativa, della risposta alle emergenze e delle esercitazioni di ripristino.

4.2. Responsabile della continuità operativa

4.2.1. È responsabile dello sviluppo e del mantenimento dei BCP a livello organizzativo e del coordinamento dei test di continuità.

4.2.2. Mantiene il piano delle BIA, facilita la formazione e garantisce che la documentazione soddisfi gli standard di conformità.

[... 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. La presente politica deve essere riesaminata annualmente dal Responsabile della continuità operativa e dal CISO per garantirne l'allineamento con:

9.1.1. Modifiche nelle operazioni aziendali, nei sistemi critici o nell'infrastruttura

9.1.2. Lezioni apprese da incidenti, audit, esercitazioni tabletop o test DR

9.1.3. Obblighi normativi o contrattuali aggiornati (ad esempio DORA, GDPR, requisiti RTO/RPO dei clienti)

9.1.4. Modifiche alla propensione al rischio dell'organizzazione o alla strategia di continuità operativa

9.2. I riesami devono includere:

9.2.1. Verifica dell'adeguatezza dei piani e dei recapiti di contatto

9.2.2. Rivalutazione di RTO, RPO e classificazione dei livelli di ripristino

9.2.3. Valutazione della capacità dei servizi di backup e disaster recovery

9.2.4. Feedback dei portatori di interesse che hanno eseguito piani di ripristino o test recenti

9.3. Tutte le modifiche alla politica devono essere:

9.3.1. Gestite con controllo di versione, motivazione documentata e approvazione dei portatori di interesse

9.3.2. Comunicate al personale e ai team chiave con responsabilità aggiornate

9.3.3. Recepita nei materiali di formazione, sensibilizzazione e nelle procedure operative aggiornate

9.4. Devono essere emessi aggiornamenti intermedi urgenti in caso di cambiamento organizzativo rilevante, obbligo di legge o rilievo critico che renda i piani o la politica vigente non più praticabili.

10. Politiche correlate e collegamenti

10.1. La presente politica opera in coordinamento con i seguenti documenti chiave:

10.1.1. P1 – Politica per la sicurezza delle informazioni: stabilisce il requisito di operazioni resilienti basate sul rischio in ogni condizione.

10.1.2. P5 – Politica di change management: garantisce che qualsiasi modifica di configurazione o infrastruttura connessa al ripristino segua flussi documentati e approvati.

10.1.3. P14 – Politica di conservazione e smaltimento dei dati: disciplina il ciclo di vita dei supporti di backup e dei dati ripristinati utilizzati nelle operazioni di continuità.

10.1.4. P15 – Politica di backup e ripristino: applica controlli sulla frequenza dei backup, sulla sicurezza e sulla verifica del ripristino.

10.1.5. P18 – Politica sui controlli crittografici: garantisce che i processi di ripristino rispettino gli standard di cifratura e riservatezza.

10.1.6. P22 – Politica di logging e monitoraggio: supporta il rilevamento e l'escalation degli eventi che incidono sulla continuità operativa.

10.1.7. P30 – Politica di risposta agli incidenti: definisce i processi di contenimento, escalation e analisi della causa radice in coerenza con gli attivatori della continuità operativa.

10.1.8. P33 – Politica di audit e monitoraggio della conformità: verifica l'integrità e l'efficacia delle pratiche di continuità operativa e ripristino nei sistemi e nei processi.

11. Standard e quadri di riferimento

11.1. La presente politica è allineata a standard internazionalmente riconosciuti in materia di continuità operativa e disaster recovery, a supporto dell'auditabilità, della resilienza e della conformità legale.

11.2. ISO/IEC 27002

11.2.1. Allegato A, controllo 5.29 – Sicurezza delle informazioni durante le interruzioni: richiede la continuità dei controlli di sicurezza in condizioni avverse.

11.2.2. Allegato A, controllo 5.30 – Prontezza ICT per la continuità operativa: richiede la preparazione, il test e la validazione delle capacità di ripristino ICT.

11.3. ISO 22301:2019 – Sistemi di gestione della continuità operativa

11.3.1. Fornisce il quadro di riferimento per stabilire, attuare e mantenere pratiche di BCM allineate agli obiettivi organizzativi e alle soglie di rischio.

11.4. NIST SP 800-34 Rev.1 – Guida alla pianificazione della continuità operativa

11.4.1. Definisce le migliori pratiche per i piani di continuità dei sistemi IT, incluse la definizione della strategia di continuità operativa, l'analisi d'impatto e il test dei piani.

11.5. GDPR UE (2016/679)

11.5.1. Articolo 32 – Sicurezza del trattamento: richiede la resilienza dei sistemi e dei servizi di trattamento e il tempestivo ripristino della disponibilità e dell'accesso ai dati personali a seguito di un incidente.

11.6. Direttiva UE NIS2 (2022/2555)

11.6.1. Articolo 21(2)(f): richiede misure di continuità operativa e gestione delle crisi a supporto della sicurezza delle reti e dei sistemi informativi.

11.7. Regolamento UE DORA (2022/2554)

11.7.1. Articolo 10 – Continuità operativa ICT: richiede che i soggetti finanziari sviluppino e testino piani di continuità ICT, inclusi RTO/RPO basati sul rischio e capacità di failover.

11.8. COBIT 2019

11.8.1. DSS04 – Gestire la continuità: copre tutti gli aspetti della pianificazione della continuità, inclusi identificazione delle minacce, analisi d'impatto, strategia di ripristino e test periodici.