					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P15					Titolo del documento: **Politica di backup e ripristino**							
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**

Allineata a norme e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 6.1.3, 8.1	Trattamento del rischio, pianificazione e controlli operativi di backup
ISO/IEC 27002:2022	Controlli 8.13, 5.28, 5.29	Gestione dei backup, smaltimento sicuro e resilienza
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Requisiti per il backup dei sistemi, il ripristino e la sanitizzazione dei supporti
GDPR UE	Articolo 32, Considerando 49	Ripristino e disponibilità dei dati personali, continuità operativa
NIS2 UE	Articolo 21(2)(c-e)	Controlli di backup e continuità a supporto della resilienza
DORA UE	Articoli 10, 11	Requisiti di backup, ripristino e test per il settore finanziario
COBIT 2019	DSS01, DSS04, MEA03	Operazioni di backup, continuità e monitoraggio della conformità

1. Finalità

1.1 La presente politica definisce i requisiti obbligatori per il backup e il ripristino di dati, sistemi e applicazioni, a supporto della resilienza operativa, dell'integrità dei dati e della continuità operativa.

1.2 La politica stabilisce un quadro di riferimento standardizzato per:

1.2.1 Proteggere i dati dell'organizzazione dalla perdita dovuta a cancellazione, corruzione, guasti o attacchi informatici

1.2.2 Definire i requisiti di ripristino attraverso parametri chiari di RTO (Recovery Time Objective) e RPO (Recovery Point Objective)

1.2.3 Integrare le operazioni di backup con il più ampio SGSI e con i piani di continuità operativa (BCP/DRP)

1.2.4 Garantire la conformità alle leggi applicabili e ai regolamenti di settore in materia di disponibilità e recuperabilità

1.3 La politica attua i controlli della ISO/IEC 27001:2022 relativi allo smaltimento sicuro dei dati (5.28), alla resilienza (5.29) e al backup delle informazioni (8.13), ed è allineata alle buone pratiche di ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR, DORA e NIS2.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutti i sistemi critici per l'operatività e i sistemi in esercizio compresi nel campo di applicazione del SGSI

2.1.2 Tutti i dati aziendali strutturati e non strutturati, inclusi database, file, e-mail e configurazioni

2.1.3 Tutti gli ambienti — on-premise, cloud, ibridi e archiviazione remota/fuori sede

2.1.4 Tutto il personale responsabile della gestione, dell'esecuzione, della verifica o del ripristino dei processi di backup

2.2 Si applica inoltre a:

2.2.1 Supporti e infrastruttura di backup, inclusi nastri fisici, appliance virtuali, snapshot disco e soluzioni di backup cloud

2.2.2 Fornitori terzi incaricati di ospitare, gestire o trattare i backup dell'organizzazione

2.2.3 Backup di log, configurazioni, tracce di audit e documentazione operativa critica per la continuità

2.3 I sistemi esplicitamente esclusi dal backup devono essere documentati, sottoposti a valutazione del rischio e formalmente approvati dal Responsabile del SGSI e dal proprietario del sistema.

3. Obiettivi

3.1 Garantire che tutti i sistemi e i dati critici siano sottoposti a backup in modo affidabile, con frequenza, ridondanza e controlli di sicurezza adeguati.

3.2 Fornire meccanismi di ripristino che soddisfino i requisiti definiti di RTO e RPO in coerenza con le valutazioni di impatto sul business.

3.3 Mantenere una documentazione completa delle procedure di backup, dei tempi di conservazione, dei ruoli e delle tecnologie utilizzate.

3.4 Convalidare l'efficacia delle operazioni di backup mediante test sistematici di ripristino, registrazione dei guasti e tracciamento delle azioni correttive.

3.5 Proteggere i dati di backup da accessi non autorizzati, modifica o distruzione per l'intero ciclo di vita.

3.6 Garantire la conformità a:

3.6.1 Requisiti dei controlli operativi e di continuità della ISO/IEC 27001

3.6.2 Famiglie CP e MP del NIST SP 800-53 per backup e sanitizzazione

3.6.3 Articolo 32 e Considerando 49 del GDPR per il ripristino dell'accesso ai dati personali

3.6.4 Articolo 10 del DORA e Articolo 21 della NIS2 per continuità e resilienza dei sistemi ICT

3.7 Garantire che i servizi di backup erogati da terze parti soddisfino gli obblighi contrattuali e regolatori in materia di sicurezza, inclusi cifratura, smaltimento e protocolli di notifica.

4. Ruoli e responsabilità

4.1 Direzione aziendale

4.1.1 Approva la presente politica e garantisce che i sistemi critici per l'operatività siano adeguatamente protetti mediante pratiche di backup e ripristino approvate.

4.1.2 Assicura che le operazioni di backup dispongano di risorse adeguate e siano riesaminate periodicamente ai fini della conformità normativa.

4.2 Responsabile della sicurezza delle informazioni (CISO)

4.2.1 È il titolare della politica e ne garantisce l'allineamento con il più ampio quadro di riferimento in materia di sicurezza delle informazioni, rischio e continuità.

4.2.2 Supervisiona l'integrazione delle procedure di backup nei BCP/DRP, nella gestione degli incidenti e nella pianificazione della resilienza.

4.2.3 Riesamina le eccezioni relative al backup e valuta le proposte di accettazione del rischio per l'esclusione di sistemi 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 La presente politica deve essere riesaminata almeno una volta l'anno, o prima se determinato da:

9.1.1 Modifiche nella strategia di continuità operativa o di disaster recovery

9.1.2 Nuovi obblighi normativi o legali che incidano sulla frequenza dei backup o sulla conservazione dei dati

9.1.3 Modifiche dell'architettura dei sistemi, degli strumenti di backup o dei fornitori di servizi

9.1.4 Incidenti significativi o risultanze di audit relative a perdita di dati o guasti nel recupero

9.2 Il riesame deve essere coordinato dal CISO in collaborazione con:

9.2.1 Infrastruttura e Operazioni IT

9.2.2 Audit interno

9.2.3 Responsabile della protezione dei dati (DPO)

9.2.4 Team di continuità operativa e disaster recovery

9.3 Le pianificazioni di backup, gli elenchi dei sistemi inclusi, la documentazione di ripristino e i registri delle eccezioni devono essere riesaminati in parallelo per garantire:

9.3.1 L'accuratezza della copertura di backup per tutti gli asset critici

9.3.2 La conformità ai requisiti di RTO/RPO e conservazione

9.3.3 La completezza dei log di test e delle segnalazioni di incidente

9.3.4 La correzione delle lacune nei controlli precedentemente identificate

9.4 Tutti gli aggiornamenti devono:

9.4.1 Essere sottoposti a controllo di versione e conservati nel repository documentale del SGSI

9.4.2 Includere un riepilogo delle modifiche e la relativa giustificazione

9.4.3 Essere approvati dalla Direzione aziendale

9.4.4 Essere comunicati a tutto il personale tecnico e aziendale interessato

10. Politiche correlate e collegamenti

10.1 La presente politica supporta direttamente e interagisce con i seguenti documenti correlati:

10.1.1 P6 - Politica di gestione del rischio: identifica la prioritizzazione basata sul rischio della protezione dei backup per sistemi e servizi.

10.1.2 P12 - Politica di gestione degli asset: garantisce che i sistemi soggetti a backup siano inclusi nell'inventario e collegati al tracciamento del ciclo di vita e alla classificazione.

10.1.3 P13 - Politica di classificazione ed etichettatura dei dati: definisce quali categorie di dati richiedono backup, inclusi i metadati di etichettatura per la prioritizzazione.

10.1.4 P14 - Politica di conservazione e smaltimento dei dati: coordina la conservazione dei backup con i limiti normativi di conservazione e il corretto smaltimento dei supporti scaduti.

10.1.5 P16 - Politica di mascheramento dei dati e pseudonimizzazione: supporta la minimizzazione dei dati durante il backup di insiemi di dati sensibili.

10.1.6 P30 - Politica di risposta agli incidenti (P30): viene attivata in caso di guasti del backup, problemi di ripristino o compromissione dei repository dei dati di backup.

10.2 Tali politiche interconnesse costituiscono un quadro di riferimento coerente che garantisce l'integrazione della governance del backup nel più ampio SGSI dell'organizzazione e nella strategia di resilienza operativa.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001:

11.1.1 Clausola 6.1.3 - Piano di trattamento del rischio: supporta la prioritizzazione del backup basata sul rischio e la pianificazione del ripristino.

11.1.2 Clausola 8.1 - Pianificazione e controllo operativi: integra i controlli di recupero e continuità come parte delle misure di sicurezza operative.

11.1.3 Allegato A Controllo 5.28 - Smaltimento sicuro o riutilizzo delle apparecchiature: disciplina la sanitizzazione sicura dei supporti di backup.

11.1.4 Allegato A Controllo 5.29 - Sicurezza delle informazioni durante l'interruzione: garantisce capacità di ripristino durante incidenti o disastri.

11.1.5 Allegato A Controllo 8.13 - Backup delle informazioni: è attuato direttamente mediante operazioni di backup pianificate, testate e sicure.

11.2 ISO/IEC 27002:2022 - Controlli 8.13, 5.28, 5.29: tali controlli rafforzano il requisito di backup regolari, convalida dell'integrità e pianificazione del ripristino in tutti gli ambienti IT.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Backup di sistema: stabilisce procedure di backup complete, inclusi archiviazione fuori sede e test di ripristino.

11.3.2 CP-10 - Recupero e ripristino del sistema: richiede procedure convalidate per il ripristino completo o parziale in linea con gli obiettivi di recupero.

11.3.3 MP-6 - Sanitizzazione dei supporti: garantisce la gestione sicura dei supporti di backup obsoleti.

11.3.4 SI-12 - Procedure di gestione delle informazioni: rafforza le responsabilità di backup e recupero per i dati sensibili.

11.4 GDPR UE (2016/679):

11.4.1 Articolo 32 - Sicurezza del trattamento: impone capacità di ripristino e misure di protezione della disponibilità dei dati, in particolare per i dati personali.

11.4.2 Considerando 49: supporta le misure di continuità operativa e disaster recovery, incluso il backup sicuro quale parte della resilienza organizzativa.

11.5 Direttiva UE NIS2 (2022/2555):

11.5.1 Articolo 21(2)(c-e): richiede misure tecniche e organizzative, inclusi controlli di backup e continuità, per garantire la resilienza dei servizi.

11.6 DORA UE (2022/2554):

11.6.1 Articolo 10 - Continuità operativa ICT: richiede che i soggetti finanziari dispongano di backup completi dei dati, capacità di recupero e pianificazione della continuità.

11.6.2 Articolo 11 - Test dei piani di continuità operativa ICT: pone l'accento sulla convalida delle capacità di recupero mediante test regolari.

11.7 COBIT 2019:

11.7.1 DSS01 - Managed Operations: supporta l'erogazione affidabile dei servizi attraverso la protezione della disponibilità dei dati.

11.7.2 DSS04 - Managed Continuity: definisce controlli strategici e operativi di continuità, inclusi backup verificati.

11.7.3 MEA03 - Monitor, Evaluate, and Assess Compliance: richiede il riesame periodico delle misure di continuità, inclusa l'efficacia dei controlli di backup.