					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P30					Titolo del documento: **Politica di risposta agli incidenti**							
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 regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8.1, Clausola 9	Processi strutturati per la gestione del rischio e la risposta agli incidenti
ISO/IEC 27002:2022	Controlli 5.25–5.27	Ruoli, segnalazione, risposta e miglioramento nella gestione degli incidenti
NIST SP 800-53 Rev.5	IR-1 fino a IR-9	Ciclo di vita completo della risposta agli incidenti
GDPR UE	Articolo 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Tempistiche di notifica della violazione, segnalazione e comunicazione agli interessati
NIS2 UE	Articolo 23(1)–(4)	Notifica all'autorità nazionale e segnalazione strutturata
DORA UE	Articolo 17(1)–(3)	Segnalazione dei gravi incidenti ICT per le entità finanziarie
COBIT 2019	DSS02, DSS04, MEA	Definizione, monitoraggio e valutazione della gestione degli incidenti, della continuità operativa e delle attività di valutazione

1. Finalità

1.1 La presente politica definisce un quadro formale per l'identificazione, la segnalazione, l'analisi, il contenimento, la risposta, il ripristino e la valutazione post-incidente degli incidenti di sicurezza delle informazioni che interessano l'organizzazione.

1.2 Essa assicura una risposta tempestiva, coordinata ed efficace al fine di ridurre al minimo l'interruzione operativa, le perdite finanziarie, il danno reputazionale e la non conformità normativa.

1.3 La politica promuove inoltre il miglioramento continuo della postura di resilienza informatica dell'organizzazione attraverso le lezioni apprese e l'integrazione delle risultanze post-incidente nella governance, negli strumenti e nei programmi di formazione.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 tutto il personale, inclusi dipendenti, collaboratori esterni, consulenti e fornitori di servizi terzi

2.1.2 tutti i sistemi informativi, le applicazioni, l'infrastruttura IT, le reti e i dati, sia on-premise sia in cloud o in ambienti ibridi

2.1.3 tutte le tipologie di incidenti di sicurezza, inclusi, a titolo esemplificativo e non esaustivo:

2.1.3.1 accesso non autorizzato o elevazione dei privilegi

2.1.3.2 attacchi malware e ransomware

2.1.3.3 attacchi di denial-of-service (DoS/DDoS)

2.1.3.4 perdita, divulgazione o esfiltrazione di dati

2.1.3.5 uso improprio interno o violazioni della politica

2.1.3.6 violazioni della sicurezza fisica che impattano gli asset digitali

2.2 La politica comprende rilevazione, triage, indagine, escalation, contenimento, gestione delle evidenze, notifica, ripristino e analisi della causa radice.

3. Obiettivi

3.1 Istituire una capacità di risposta agli incidenti ripetibile e scalabile che consenta il rilevamento, la classificazione e la mitigazione tempestivi degli incidenti di sicurezza.

3.2 Ridurre al minimo l'impatto operativo degli eventi di sicurezza attraverso procedure strutturate di contenimento, eradicazione e ripristino dei sistemi.

3.3 Garantire che la segnalazione e la risposta agli incidenti siano allineate ai requisiti legali, normativi e contrattuali, in particolare a quelli relativi alle tempistiche di notifica delle violazioni e alla gestione delle evidenze.

3.4 Supportare la trasparenza e l'accountability mediante adeguata registrazione, documentazione e tracciamento delle metriche per tutti gli incidenti di sicurezza.

3.5 Promuovere il miglioramento continuo attraverso riesami post-incidente, azioni correttive e formazione delle parti interessate.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO)

4.1.1 È responsabile del quadro di riferimento per la risposta agli incidenti, assicura l'applicazione della politica e sovraintende al coordinamento degli incidenti a livello aziendale.

4.1.2 Agisce quale principale punto di raccordo con le autorità di regolamentazione, il vertice aziendale e il consulente legale esterno durante gli incidenti rilevanti.

4.2 Coordinatore della risposta agli incidenti

4.2.1 Coordina i team di risposta interfunzionali, gestisce i flussi di lavoro e monitora lo stato delle attività di contenimento e ripristino.

4.2.2 Attiva e conduce i riesami post-incidente e assicura che le azioni correttive siano registrate e attuate.

[... 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 annualmente e aggiornata, se necessario, per recepire:

9.1.1 cambiamenti nel panorama delle minacce, nelle tipologie di incidente o nei vettori di attacco

9.1.2 lezioni apprese da incidenti rilevanti, quasi incidenti o risultanze delle autorità di regolamentazione

9.1.3 aggiornamenti delle leggi e dei regolamenti applicabili (ad es. GDPR, DORA, NIS2)

9.1.4 feedback derivanti dalle esercitazioni di risposta agli incidenti e dai riesami post-incidente

9.2 Il CISO è responsabile dell'avvio e del coordinamento del processo di riesame, in consultazione con:

9.2.1.1 consulente legale e DPO

9.2.1.2 SOC e operazioni IT

9.2.1.3 team di continuità operativa e gestione del rischio

9.2.1.4 direzione aziendale

9.3 Le modifiche alla politica devono essere:

9.3.1 documentate in un repository soggetto a controllo di versione

9.3.2 comunicate a tutti i team interessati e recepite nella formazione di sensibilizzazione

9.3.3 convalidate mediante esercitazioni tabletop o live di risposta agli incidenti entro tre mesi dall'approvazione

9.4 Gli aggiornamenti urgenti determinati da rischi emergenti, risultanze dell'audit o nuovi obblighi legali devono essere adottati immediatamente e registrati nella cronologia delle versioni della politica.

10. Politiche correlate e collegamenti

10.1 La presente politica è supportata dalle seguenti politiche organizzative e dipende da esse:

10.1.1 P1 – Politica per la sicurezza delle informazioni: stabilisce il requisito generale per operazioni basate sul rischio e pronte alla gestione degli incidenti.

10.1.2 P5 – Politica di gestione delle modifiche: assicura che le attività di contenimento e ripristino che coinvolgono infrastruttura o servizi seguano procedure formali.

10.1.3 P13 – Politica di classificazione ed etichettatura dei dati: supporta la classificazione della gravità degli incidenti in base alla sensibilità dei dati.

10.1.4 P15 – Politica di backup e ripristino: consente il ripristino da ransomware o attacchi distruttivi con garanzia di integrità.

10.1.5 P18 – Politica sui controlli crittografici: definisce le misure di cifratura che riducono l'impatto dell'incidente e i rischi di esposizione dei dati.

10.1.6 P22 – Politica di registrazione e monitoraggio: fornisce la visibilità di base sugli eventi, l'allertamento e la conservazione dei log necessari per un rilevamento efficace e per le attività forensi.

10.1.7 P29 – Politica sui dati di test e sugli ambienti di test: assicura che anche gli incidenti che coinvolgono sistemi non produttivi siano gestiti in modo strutturato e sicuro.

10.1.8 P33 – Politica di monitoraggio dell'audit e della conformità: convalida la preparazione agli incidenti e l'efficacia della risposta attraverso audit strutturati e valutazioni di conformità.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001: Clausola 8.1 – Pianificazione e controllo operativi: processi strutturati per gestire i rischi e pianificare la risposta agli incidenti.

11.2 ISO/IEC 27002:2022 – Controlli 5.25–5.27: responsabilità per la gestione degli incidenti, la segnalazione, la risposta, la comunicazione e il miglioramento.

11.3 NIST SP 800-53 Rev.5: IR-1 fino a IR-9, AU-6, PL-2: requisiti completi per il ciclo di vita della risposta agli incidenti, l'audit e la pianificazione della sicurezza.

11.4 GDPR UE: Articoli 33/34: obblighi di notifica alle autorità di controllo e requisiti di comunicazione agli interessati (con eccezioni definite).

11.5 Direttiva UE NIS2 (2022/2555): Articolo 23: segnalazione nazionale obbligatoria, con obblighi di segnalazione intermedia e finale.

11.6 DORA UE (2022/2554): Articolo 17: requisiti di segnalazione alle autorità per gli incidenti ICT delle istituzioni finanziarie.

11.7 COBIT 2019: DSS02, DSS04, MEA01: gestione degli incidenti di servizio e della continuità operativa, oltre al monitoraggio delle prestazioni e della conformità.