					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P30S					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 norme e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 6.1, 6.3, 8	Gestione degli incidenti, miglioramento continuo, controllo operativo
ISO/IEC 27002:2022	Controlli 5.24, 5.25	Rilevazione degli incidenti, preparazione, apprendimento
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Gestione dell'incidente, monitoraggio e segnalazione
GDPR UE	Articolo 33	Requisiti di notifica delle violazioni
NIS2 UE	Articolo 23	Obbligo di segnalazione degli incidenti informatici
DORA UE	Articolo 17	Gestione degli incidenti ICT
COBIT 2019	DSS02, DSS04	Gestione dei servizi e degli incidenti, continuità operativa

1. Finalità

1.1. La presente politica definisce le modalità con cui l'organizzazione rileva, segnala e gestisce la risposta agli incidenti di sicurezza delle informazioni che coinvolgono i propri sistemi digitali, dati o servizi.

1.2. La politica consente all'organizzazione di minimizzare i danni, proteggere i dati dei clienti e adempiere agli obblighi normativi, incluso l'obbligo previsto dal GDPR di notificare le violazioni entro 72 ore.

1.3. La politica assicura chiarezza in merito a responsabilità, flussi di comunicazione e attività di follow-up successive all'incidente, anche nelle organizzazioni di piccole dimensioni prive di un team di sicurezza dedicato.

2. Ambito di applicazione

2.1. La presente politica si applica a:

2.1.1. Tutti i dipendenti, i collaboratori esterni e i fornitori di servizi IT

2.1.2. Tutti i sistemi e i servizi gestiti dall'azienda, inclusi siti web, piattaforme cloud, dispositivi mobili, laptop e account di posta elettronica

2.1.3. Tutte le tipologie di incidente, inclusi:

2.1.3.1. Accesso non autorizzato a dati o sistemi

2.1.3.2. Infezioni da malware o ransomware

2.1.3.3. Tentativi di phishing o ingegneria sociale

2.1.3.4. Indisponibilità dei sistemi dovuta ad attacco informatico o uso improprio

2.1.3.5. Divulgazione accidentale o cancellazione di informazioni sensibili

2.1.3.6. Smarrimento o furto di dispositivi aziendali o supporti di archiviazione

3. Obiettivi

3.1. Stabilire un processo chiaro per il riconoscimento e l'escalation degli incidenti di sicurezza.

3.2. Assicurare che gli incidenti siano segnalati, registrati e gestiti entro tempi prestabiliti.

3.3. Consentire il rapido contenimento del danno, il recupero dei dati e il ripristino dei servizi.

3.4. Assicurare che le parti interessate coinvolte, ad esempio clienti e autorità di regolamentazione, siano informate quando richiesto dalla legge.

3.5. Prevenire il ripetersi degli incidenti mediante analisi delle cause radice, azioni correttive e aggiornamento della politica.

3.6. Consentire alle piccole e medie imprese (PMI) di soddisfare i requisiti di certificazione ISO/IEC 27001 e dimostrare la propria accountability in sede di audit.

4. Ruoli e responsabilità

4.1. Direttore generale (GM)

4.1.1. È il titolare della politica e ne assicura l'attuazione.

4.1.2. Sovrintende alle attività di risposta agli incidenti e approva le notifiche alle autorità di regolamentazione o ai clienti.

4.1.3. Riesamina i rapporti post-incidente e assicura l'aggiornamento della politica quando necessario.

4.1.4. Può delegare le attività di coordinamento, mantenendo comunque la responsabilità complessiva.

4.2. Fornitore IT / Amministratore di sistema (interno o esterno)

4.2.1. Rileva e analizza i potenziali incidenti di sicurezza.

4.2.2. Attua le azioni di contenimento e ripristino, ad esempio disabilitazione degli accessi e ripristino dei backup.

4.2.3. Notifica al GM tutti gli incidenti confermati o sospetti entro 1 ora dalla rilevazione.

4.2.4. Mantiene un registro degli incidenti con marca temporale, valutazione dell'impatto e azioni di risposta.

[... 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 programmato

9.1.1. La presente politica deve essere riesaminata almeno una volta ogni 12 mesi dal Direttore generale (GM) per assicurare:

9.1.1.1. L'allineamento ai controlli ISO/IEC 27001:2022

9.1.1.2. La capacità di risposta a nuove minacce, rischi e incidenti

9.1.1.3. Il mantenimento della conformità agli obblighi legali e contrattuali, ad esempio GDPR e DORA

9.2. Eventi attivanti

9.2.1. La politica deve inoltre essere riesaminata e aggiornata dopo:

9.2.1.1. Qualsiasi incidente ad alta gravità o notifica a un'autorità di regolamentazione

9.2.1.2. L'introduzione di nuova infrastruttura IT o modifiche ai sistemi

9.2.1.3. Modifiche ai requisiti di legge relativi alle violazioni della sicurezza

9.3. Documentazione del riesame e distribuzione

9.3.1. Tutti i riesami e le modifiche devono essere documentati nel registro delle modifiche della politica

9.3.2. Le versioni aggiornate devono essere distribuite a tutti i dipendenti, fornitori e fornitori IT coinvolti nella sicurezza o nelle operazioni sui sistemi

9.3.3. Le evidenze della consapevolezza del personale, ad esempio note di riunione o conferme via e-mail, devono essere conservate per dimostrare la conformità in sede di audit

10. Politiche correlate e collegamenti

10.1. La presente politica deve essere applicata in coordinamento con le seguenti politiche SME:

10.1.1. P1S – Politica per la sicurezza delle informazioni: definisce le aspettative generali per il mantenimento di riservatezza, integrità e disponibilità (CIA) durante le operazioni, inclusa la gestione degli incidenti.

10.1.2. P2S – Politica sui ruoli e le responsabilità di governance: definisce le strutture di autorità e responsabilità per la rilevazione, la segnalazione e l'escalation degli incidenti.

10.1.3. P4S – Politica di controllo degli accessi: consente la revoca immediata dei diritti di accesso durante le azioni di risposta agli incidenti.

10.1.4. P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: assicura che tutti i dipendenti siano in grado di identificare e segnalare efficacemente gli incidenti di sicurezza.

10.1.5. P17S – Politica di protezione dei dati e privacy: disciplina le procedure legali di notifica delle violazioni ai sensi del GDPR e supporta la conformità normativa durante gli incidenti.

10.1.6. P22S – Politica di logging e monitoraggio: fornisce gli strumenti e la visibilità necessari per rilevare, analizzare e sottoporre a audit gli eventi di sicurezza.

10.1.7. P31S – Politica sulla raccolta delle evidenze e analisi forense: supporta le indagini e la sostenibilità giuridica delle azioni correlate agli incidenti, guidando la corretta gestione delle evidenze.

10.2. Tali politiche definiscono congiuntamente il quadro operativo della PMI per rilevare, gestire la risposta e ripristinare i servizi in caso di incidenti di sicurezza delle informazioni.

11. Standard e quadri di riferimento

11.1. ISO/IEC 27001

11.1.1. Clausola 6.1 – Richiede la pianificazione del trattamento del rischio, inclusa la preparazione agli incidenti.

11.1.2. Clausola 6.3 – Supporta il miglioramento continuo attraverso le lezioni apprese dagli eventi di sicurezza.

11.1.3. Clausola 8.1 – Enfatizza il controllo operativo per la gestione degli incidenti e delle interruzioni.

11.2. ISO/IEC 27002

11.2.1. Controllo 5.24 – Richiede un approccio strutturato per la segnalazione, la valutazione e la risposta agli incidenti di sicurezza delle informazioni.

11.2.2. Controllo 5.25 – Si concentra sull'apprendimento dagli incidenti per migliorare la preparazione futura e la resilienza dei sistemi.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Definisce le procedure di gestione dell'incidente, inclusi contenimento e ripristino.

11.3.2. IR-5 – Stabilisce i requisiti per il monitoraggio e l'analisi degli incidenti.

11.3.3. IR-6 – Impone protocolli di segnalazione degli incidenti interni ed esterni.

11.4. GDPR UE

11.4.1. Articolo 33 – Richiede la notifica delle violazioni dei dati personali alle autorità di regolamentazione entro 72 ore, con dettagli su ambito e mitigazione.

11.5. Direttiva UE NIS2 (2022/2555)

11.5.1. Articolo 23 – Richiede ai soggetti essenziali e importanti di notificare gli incidenti significativi alle autorità competenti utilizzando formati di segnalazione standardizzati.

11.6. Regolamento UE DORA (2022/2554)

11.6.1. Articolo 17 – Richiede ai soggetti finanziari di classificare, segnalare e tracciare gli incidenti e le interruzioni correlati ai sistemi ICT.

11.7. COBIT 2019

11.7.1. DSS02 – Gestire le richieste di servizio e gli incidenti: fornisce indicazioni per una gestione efficace degli incidenti operativi e di sicurezza in linea con gli obiettivi di governance.

11.7.2. DSS04 – Gestire la continuità: collega la risposta agli incidenti a strategie più ampie di continuità operativa e ripristino.