					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P31S					Titolo del documento: **Politica P31S per la raccolta delle evidenze e l'analisi forense**							
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	Pianificazione basata sul rischio, azioni di miglioramento e controlli operativi per l'integrità delle evidenze
ISO/IEC 27002:2022	Controlli 5.24–5.27	Fornisce indicazioni per il trattamento sicuro, i riesami post-incidente e i miglioramenti basati sulle evidenze
ISO/IEC 27035-3:2016	Clausole 6.3, 6.4, 7	Garantisce un'adeguata pianificazione, la raccolta lecita e il trattamento sicuro delle evidenze digitali con documentazione della catena di custodia
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Preparazione forense, protezione dei log di audit ed efficace integrazione nella risposta agli incidenti
GDPR UE	Articoli 33, 34	Documentazione e tracciabilità per le violazioni dei dati personali
NIS2 UE	Articolo 23	Segnalazione tracciabile degli incidenti e trattamento sicuro delle evidenze
DORA UE	Articolo 17(1), 17(2)	Garantisce la raccolta, l'archiviazione e la conservazione delle evidenze per gli incidenti correlati alle ICT, la solidità forense e le richieste delle autorità di regolamentazione
COBIT 2019	DSS05.06, DSS05.07	Registrazione affidabile e trattamento strutturato delle evidenze per indagini sicure e verificabili

1. Finalità

1.1. La presente politica definisce le modalità con cui l'organizzazione gestisce le evidenze digitali relative a incidenti di sicurezza, violazioni dei dati o indagini interne. Garantisce che le evidenze siano raccolte, archiviate e conservate in modo giuridicamente sostenibile e che siano disponibili, su richiesta, in sede di audit, a supporto sia del processo decisionale interno sia di eventuali azioni esterne.

1.2. La politica consente alle piccole organizzazioni di proteggere l'integrità di log, file e immagini di sistema, dimostrando la due diligence ai sensi della ISO/IEC 27001, del GDPR e delle normative correlate.

1.3. Supporta la preparazione forense senza richiedere risorse tecniche avanzate o un team IT dedicato a tempo pieno, definendo con chiarezza ruoli, processi e requisiti di conservazione.

2. Ambito di applicazione

2.1. La presente politica si applica a:

2.1.1. Tutti i dipendenti, i fornitori di servizi IT e i consulenti esterni coinvolti nella risposta agli incidenti, nelle indagini o nell'analisi delle violazioni

2.1.2. Tutti i sistemi aziendali, inclusi laptop, dispositivi mobili, server, account e-mail, piattaforme SaaS e archiviazione cloud (ad es. Microsoft 365, Google Workspace)

2.1.3. Qualsiasi evento che richieda evidenze per azioni disciplinari interne, difesa in giudizio, richieste assicurative o interlocuzioni con le autorità di regolamentazione

2.2. Sono inclusi sia gli eventi accertati sia quelli sospetti che riguardano:

2.2.1. Perdita di dati

2.2.2. Minacce interne o uso improprio

2.2.3. Violazioni della sicurezza (ad es. malware, accesso non autorizzato)

2.2.4. Reclami dei clienti che richiedono validazione digitale

2.2.5. Richieste delle autorità di regolamentazione o delle forze dell'ordine

3. Obiettivi

3.1. Garantire che tutte le evidenze siano raccolte e trattate in modo da mantenerne l'integrità, l'autenticità e la catena di custodia.

3.2. Prevenire modifiche accidentali, cancellazioni o trattamenti impropri di log, file o immagini di sistema che potrebbero essere necessari per le indagini.

3.3. Fornire un approccio coerente e verificabile alla gestione delle evidenze, conforme alle aspettative legali e regolamentari (ad es. notifica di violazione dei dati personali ai sensi del GDPR, tracciabilità ai sensi della NIS2).

3.4. Definire ruoli e responsabilità chiari per garantire l'acquisizione rapida, sicura e conforme alla legge delle evidenze durante gli incidenti di sicurezza.

3.5. Supportare la preparazione forense a livello di PMI, minimizzando la complessità ed evitando interruzioni delle operazioni quotidiane.

4. Ruoli e responsabilità

4.1. Direttore generale (GM)

4.1.1. Approva tutte le indagini formali che richiedono la raccolta di evidenze.

4.1.2. Riesamina e approva i rapporti sugli incidenti che comportano potenziali azioni legali o disciplinari.

4.1.3. Decide se debbano essere informati il consulente legale esterno o le autorità di regolamentazione.

4.1.4. Garantisce che la politica sia riesaminata e aggiornata regolarmente.

4.2. Fornitore di servizi IT / Amministratore di sistema

4.2.1. Raccoglie e conserva le evidenze digitali nel rispetto di procedure sicure.

4.2.2. Documenta marcature temporali, dettagli di sistema e fasi del trattamento.

4.2.3. Protegge tutti i materiali raccolti in una posizione sicura.

4.2.4. Supporta l'analisi forense, se necessario.

[... 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

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

9.1.1.1. La conformità ai controlli dell'Allegato A della ISO/IEC 27001

9.1.1.2. La perdurante rilevanza rispetto alle attuali piattaforme digitali e ai servizi IT

9.1.1.3. L'adeguatezza delle procedure di registrazione, conservazione delle evidenze e preparazione forense

9.2. Eventi attivanti per la revisione della politica

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

9.2.1.1. Qualsiasi incidente rilevante che richieda la raccolta di evidenze

9.2.1.2. Un audit non superato o una richiesta regolamentare in cui sia stata messa in dubbio l'integrità delle evidenze

9.2.1.3. L'adozione di nuovi strumenti o procedure per la risposta agli incidenti o il monitoraggio dei sistemi

9.2.1.4. Modifiche normative (ad es. aggiornamenti del GDPR o degli orientamenti NIS2)

9.3. Approvazione e distribuzione delle modifiche

9.3.1. Tutte le modifiche devono essere riesaminate e approvate dal GM

9.3.2. La versione aggiornata deve essere condivisa con:

9.3.2.1. Fornitori di servizi IT e consulenti coinvolti nelle indagini

9.3.2.2. Qualsiasi membro del personale con responsabilità di amministrazione dei sistemi

9.3.3. Una copia aggiornata deve essere conservata nell'archivio delle politiche aziendali e condivisa con gli auditor su richiesta

10. Politiche correlate e collegamenti

10.1. La presente politica è interdipendente con le seguenti politiche allineate alle PMI:

10.1.1. P2S – Politica sui ruoli e sulle responsabilità di governance: stabilisce l'autorità sulle indagini relative agli incidenti, sulle decisioni in materia di evidenze e sull'escalation legale.

10.1.2. P4S – Politica di controllo degli accessi: garantisce che solo il personale autorizzato possa accedere a sistemi e log sensibili durante le indagini.

10.1.3. P22S – Politica di registrazione e monitoraggio: fornisce i dati grezzi utilizzati come evidenze forensi e stabilisce requisiti di conservazione, controllo degli accessi e registrazione.

10.1.4. P30S – Politica di risposta agli incidenti: attiva l'esigenza di raccolta delle evidenze e definisce il flusso operativo che conduce alla conservazione forense.

10.1.5. P17S – Politica di protezione dei dati e della privacy: garantisce che tutti i dati personali raccolti come evidenze siano trattati lecitamente ai sensi del GDPR e delle normative correlate.

10.2. Tali politiche operano congiuntamente a supporto della sostenibilità giuridica, dell'integrità delle indagini e della piena preparazione agli audit ISO/IEC 27001:2022.

11. Standard e quadri di riferimento

11.1. ISO/IEC 27001

11.1.1. Clausola 6.1 – La pianificazione basata sul rischio include la prontezza alla risposta e le procedure per la gestione delle evidenze.

11.1.2. Clausola 6.3 – Supporta le azioni di miglioramento basate sulle evidenze derivanti dagli incidenti.

11.1.3. Clausola 8.1 – Richiede controlli operativi per l'integrità delle evidenze.

11.2. ISO/IEC 27002

11.2.1. Controlli 5.24–5.27 – Forniscono indicazioni per il trattamento sicuro, i riesami post-incidente e i miglioramenti basati sulle evidenze.

11.3. ISO/IEC 27035-3

11.3.1. Clausole 6.3, 6.4 e 7.3 per garantire una corretta pianificazione, la raccolta lecita e il trattamento sicuro delle evidenze digitali durante la risposta agli incidenti, inclusa la conservazione e la documentazione della catena di custodia.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 e AU-12 garantiscono la preparazione forense, la protezione dei log di audit e l'integrazione efficace della raccolta delle evidenze nel ciclo di vita della risposta agli incidenti

11.5. NIST SP 800-86

11.5.1. Definisce le migliori pratiche per acquisire, analizzare e proteggere le evidenze digitali durante la risposta agli incidenti.

11.6. GDPR UE

11.6.1. Articoli 33–34 – Richiedono documentazione e tracciabilità degli incidenti e delle evidenze nella segnalazione delle violazioni dei dati personali.

11.7. Direttiva UE NIS2 (2022/2555)

11.7.1. Articolo 23 – Richiede la segnalazione tracciabile degli incidenti e il trattamento sicuro delle evidenze per i soggetti essenziali e importanti.

11.8. DORA UE

11.8.1. Articolo 17(1) – Garantisce che le evidenze relative agli incidenti correlati alle ICT siano raccolte e archiviate in modo da supportare le indagini forensi.

11.8.2. Articolo 17(2) – Richiede che i soggetti finanziari conservino tutti i dati e i log pertinenti associati agli eventi di sicurezza, in coerenza con i requisiti di solidità forense e con le richieste delle autorità di regolamentazione.

11.9. COBIT 2019

11.9.1. DSS05.06 – Monitorare, rilevare e segnalare gli incidenti: enfatizza l'importanza di una registrazione affidabile a supporto delle indagini.

11.9.2. DSS05.07 – Indagare e intervenire sugli incidenti: richiede un trattamento strutturato delle evidenze per consentire indagini sicure e verificabili.