					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P31					Titolo del documento: **Politica di raccolta delle evidenze e 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 standard e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	
ISO/IEC 27002:2022	Controlli 5.25–5.27, 8	
ISO/IEC 27035:2016	Parti 1 e 3	
NIST SP 800-53 Rev.5	IR-1–IR-9, AU-6, PL-2	
NIST SP 800-101 Rev.1	Analisi forense di dispositivi mobili e supporti	Analisi forense di dispositivi mobili e supporti
NIST SP 800-86	Integrazione delle tecniche forensi	Integrazione delle tecniche forensi nella risposta agli incidenti
GDPR UE	Articolo 5, 33–34	
NIS2 UE	Articolo 23(1)–(4)	
DORA UE	Articolo 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Finalità

1.1 La presente politica definisce un quadro strutturato e giuridicamente sostenibile per l'identificazione, la raccolta, la conservazione, l'analisi e lo smaltimento delle evidenze digitali nel corso di incidenti di sicurezza delle informazioni effettivi o sospetti.

1.2 Essa garantisce che i processi di preparazione forense e di gestione delle evidenze:

1.2.1 mantengano l'integrità probatoria e la catena di custodia

1.2.2 supportino indagini interne, procedimenti giudiziari o segnalazioni alle autorità di regolamentazione

1.2.3 siano allineati agli standard forensi riconosciuti a livello internazionale e ai criteri di ammissibilità legale

1.3 La politica supporta l'impegno dell'organizzazione verso una risposta agli incidenti proattiva, la conformità normativa e la trasparenza della governance, riducendo al minimo l'impatto operativo.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 tutti i dipendenti, collaboratori esterni, fornitori e prestatori di servizi coinvolti nell'amministrazione dei sistemi, nella gestione degli incidenti o nelle attività investigative

2.1.2 tutti gli endpoint, i server, le applicazioni, le reti e le piattaforme cloud sotto il controllo dell'organizzazione o di sua responsabilità contrattuale

2.1.3 qualsiasi incidente o evento che richieda la gestione delle evidenze, inclusi:

2.1.3.1 minacce interne, violazioni dei dati o indagini per frode

2.1.3.2 uso improprio di sistemi o credenziali

2.1.3.3 incidenti relativi alla tecnologia operativa (OT) o ai sistemi di controllo industriale

2.1.3.4 violazioni dell'accesso fisico che coinvolgono asset digitali

2.2 La politica disciplina inoltre qualsiasi interazione con fornitori di servizi forensi di terze parti o con le forze dell'ordine nell'ambito di escalation legali o procedimenti regolatori.

3. Obiettivi

3.1 Consentire l'acquisizione rapida, sicura e conforme alla politica delle evidenze durante eventi di sicurezza o indagini.

3.2 Preservare l'integrità, l'autenticità e l'ammissibilità delle evidenze digitali raccolte mediante rigorosi controlli di accesso, registrazione e procedure di verifica.

3.3 Garantire che tutte le attività forensi siano coordinate con gli obblighi legali e regolatori, inclusi la protezione dei dati, il diritto del lavoro e le restrizioni sui trasferimenti internazionali.

3.4 Supportare l'analisi post-incidente, l'individuazione della causa radice e il miglioramento dei controlli attraverso output forensi di elevata qualità.

3.5 Integrare la preparazione forense nel Sistema di Gestione della Sicurezza delle Informazioni (SGSI), supportando audit, notifiche di violazione e decisioni della direzione aziendale.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO)

4.1.1 È il titolare della policy e garantisce che tutte le operazioni forensi siano giuridicamente sostenibili, verificabili e basate sul rischio.

4.1.2 Autorizza l'escalation verso consulenti legali esterni e fornitori di servizi forensi.

4.2 Analisti forensi / Addetti alla gestione degli incidenti

4.2.1 Conducono l'acquisizione, la conservazione e l'analisi tecnica delle evidenze.

4.2.2 Garantiscono che la catena di custodia sia registrata e mantenuta correttamente.

4.2.3 Documentano tutte le azioni, le risultanze e le configurazioni degli strumenti utilizzati durante le indagini.

[... 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 secondo necessità per riflettere:

9.1.1 modifiche a leggi, regolamenti o giurisprudenza che incidono sulle procedure forensi o sulla gestione dei dati

9.1.2 aggiornamenti agli standard forensi o agli strumenti riconosciuti dal settore

9.1.3 lezioni apprese da riesami post-incidente, contenziosi legali o risultanze di audit

9.1.4 cambiamenti tecnologici nelle piattaforme, nei dispositivi o nei sistemi oggetto di indagine

9.2 Il processo di riesame è di competenza del CISO e deve includere la consultazione di:

9.2.1 Funzione Legale e Compliance

9.2.2 Responsabile della protezione dei dati (DPO)

9.2.3 team delle operazioni di sicurezza e forense

9.2.4 Funzione di Internal Audit/Compliance

9.3 Tutte le revisioni devono essere:

9.3.1 sottoposte a controllo di versione e conservate nel repository delle policy

9.3.2 comunicate alle parti interessate coinvolte, inclusi i team forensi e di risposta

9.3.3 accompagnate da aggiornamenti delle procedure operative e dei materiali formativi pertinenti

9.4 Riesami intermedi devono essere attivati a seguito di qualsiasi incidente critico che coinvolga gestione impropria delle evidenze, interruzione della catena di custodia o problemi di ammissibilità legale.

10. Policy correlate e collegamenti

10.1 La presente politica è allineata con ed è supportata dalle seguenti policy organizzative:

10.1.1 P1 – Politica per la sicurezza delle informazioni: stabilisce il mandato di base per le indagini, il controllo delle evidenze e la conformità alle leggi applicabili.

10.1.2 P5 – Politica di gestione delle modifiche: garantisce che i sistemi oggetto di indagine non siano alterati durante i processi forensi attivi.

10.1.3 P14 – Politica di conservazione e smaltimento dei dati: disciplina lo smaltimento sicuro e i tempi di conservazione delle evidenze e dei dati relativi ai casi.

10.1.4 P18 – Politica sui controlli crittografici: definisce i requisiti di cifratura per la conservazione e il trasferimento di dati sensibili o aventi valore probatorio.

10.1.5 P22 – Politica di registrazione e monitoraggio: garantisce la disponibilità dei log degli eventi e della telemetria per la raccolta delle evidenze e la correlazione forense.

10.1.6 P30 – Politica di risposta agli incidenti (P30): definisce il triage degli incidenti e i percorsi di escalation nei quali vengono attivate le procedure forensi.

10.1.7 P33 – Politica di audit e monitoraggio della conformità: convalida il rispetto dei protocolli forensi e dei requisiti relativi alla catena di custodia attraverso audit regolari.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata agli standard internazionali in materia forense e di gestione degli incidenti, garantendo l'integrità delle evidenze, la sostenibilità giuridica e la conformità tra diverse giurisdizioni.

11.2 ISO/IEC 27001

11.2.1 Clausola 8.1 – Supporta il controllo operativo della preparazione forense e delle procedure di gestione delle evidenze

11.3 ISO/IEC 27002

11.3.1 Allegato A, Controllo 5.25 – Responsabilità per la gestione degli incidenti: richiede ruoli definiti per la gestione degli incidenti di sicurezza delle informazioni e delle indagini.

11.3.2 Allegato A, Controllo 5.26 – Segnalazione degli eventi di sicurezza delle informazioni: supporta la raccolta di artefatti relativi agli eventi come evidenze.

11.3.3 Allegato A, Controllo 5.27 – Risposta agli incidenti di sicurezza delle informazioni: impone attività di remediation e indagini strutturate e basate sulle evidenze.

11.3.4 Allegato A, Controllo 8.27 – Sviluppo sicuro e analisi forense, ove applicabile: disciplina la protezione dei sistemi e degli strumenti durante le indagini.

11.4 ISO/IEC 27035:2016 (Parti 1 e 3)

11.4.1 Delinea i principi di rilevazione degli incidenti, risposta e preparazione forense, inclusi pianificazione, catena di custodia e gestione delle evidenze dell'incidente.

11.5 NIST SP 800-53 Rev.5

11.5.1 IR-1–IR-9, AU-6, PL-2: definisce requisiti strutturati per la pianificazione, la rilevazione, l'analisi, il contenimento e la risposta agli incidenti di sicurezza. Supporta la raccolta e la verificabilità delle evidenze (AU-6) e garantisce l'allineamento con i piani di sicurezza e privacy dei sistemi (PL-2) durante le indagini forensi.

11.6 NIST SP 800-86

11.6.1 Fornisce linee guida per integrare i processi forensi nel più ampio ciclo di vita della risposta agli incidenti e garantire la preparazione forense.

11.7 NIST SP 800-101 Rev.1

11.7.1 Si concentra sulle migliori pratiche per acquisire, conservare e analizzare supporti digitali ed evidenze provenienti da dispositivi mobili in modo giuridicamente sostenibile.

11.8 GDPR UE (2016/679)

11.8.1 Articolo 5 – Principi applicabili al trattamento dei dati personali: si applica alle evidenze che contengono dati personali o dati sensibili, garantendo minimizzazione e limitazione della finalità.

11.8.2 Articoli 33–34 – Notifica della violazione dei dati personali: i dati forensi supportano la conformità agli obblighi di notifica della violazione e ai processi di divulgazione legale.

11.9 Direttiva UE NIS2 (2022/2555)

11.9.1 Articolo 23 – Obblighi di segnalazione: la documentazione forense e le risultanze supportano segnalazioni degli incidenti tempestive e accurate alle autorità competenti.

11.10 DORA UE (2022/2554)

11.10.1 Articolo 17 – Segnalazione degli incidenti ICT: richiede analisi dettagliate della causa radice e registrazioni probatorie degli incidenti ICT gravi, in particolare nel settore finanziario.

11.11 COBIT 2019

11.11.1 DSS01.07 – Gestire gli incidenti di sicurezza: impone documentazione dell'incidente e rigore investigativo.

11.11.2 DSS05.04 – Gestire le indagini di sicurezza: enfatizza la conservazione delle evidenze digitali e il supporto ad azioni disciplinari e legali.