					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P20					Titolo del documento: **Politica di protezione degli endpoint / Politica antimalware**							
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	Clausola 8	La protezione degli endpoint e i controlli antimalware sono richiesti per soddisfare gli obiettivi del SGSI
ISO/IEC 27002:2022	Controlli 8.7, 8	Fornisce controlli tecnici e linee guida per la protezione antimalware, la difesa degli endpoint e la gestione degli incidenti
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Definisce requisiti per la protezione dal codice malevolo, il monitoraggio centralizzato e la configurazione di base
Regolamento generale sulla protezione dei dati (GDPR) UE	Articolo 32	Impone misure tecniche adeguate a tutela dei dati personali, inclusa la protezione dal malware
Direttiva UE NIS2	Articolo 21(2)(d)	Richiede l'implementazione di misure di rilevazione delle minacce e di prevenzione a livello di endpoint
Regolamento UE DORA	Articolo 9	Richiede la gestione del rischio ICT relativo al malware e la difesa dalle minacce veicolate tramite endpoint
COBIT 2019	DSS05.01, DSS01.04, MEA	Richiede protezione, monitoraggio e valutazione dei controlli sugli endpoint

1. Finalità

1.1 La presente politica definisce i controlli obbligatori e i requisiti operativi per proteggere gli endpoint dell'organizzazione, inclusi desktop, laptop, dispositivi mobili e server, dal malware e dalle minacce correlate.

1.2 Stabilisce gli standard minimi per la protezione degli endpoint, il rilevamento del malware, la risposta di contenimento e il monitoraggio comportamentale, assicurando che i sistemi mantengano un'adeguata resilienza sia contro ceppi di malware comuni sia contro varianti avanzate.

1.3 La politica supporta direttamente la conformità alla clausola 8.1 della ISO/IEC 27001:2022 e al controllo 8.7 dell'Allegato A, ed è allineata agli obblighi regionali di cibersicurezza previsti da GDPR, NIS2 e DORA.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti gli endpoint, inclusi:

2.1.1 desktop, laptop, dispositivi mobili e istanze virtuali di proprietà dell'organizzazione o da essa gestiti

2.1.2 dispositivi di proprietà personale autorizzati ai sensi della politica BYOD, subordinatamente all'installazione di MDM o di un agente endpoint

2.1.3 server e asset infrastrutturali, incluse VM ospitate in cloud e dispositivi edge

2.1.4 sistemi operativi, driver, servizi locali, agenti endpoint e controlli di sicurezza installati su ciascun nodo

2.2 Rientrano nell'ambito della presente politica tutti i soggetti con responsabilità amministrative, tecniche o operative su qualsiasi endpoint, inclusi:

2.2.1 dipendenti interni e collaboratori esterni

2.2.2 Managed Service Provider (MSP), servizi esternalizzati di supporto desktop e amministratori IT di terze parti

2.2.3 utenti autorizzati a utilizzare sistemi portatili, laptop abilitati alla VPN o accesso mobile alle reti dell'organizzazione

2.3 Le minacce coperte dalla presente politica includono, a titolo esemplificativo e non esaustivo:

2.3.1 virus, worm, trojan, ransomware, spyware, rootkit, adware, keylogger, botnet

2.3.2 malware fileless, payload zero-day, malware per l'elevazione dei privilegi ed exploit kit per browser

2.3.3 codice malevolo veicolato tramite supporti rimovibili, vettori di phishing, drive-by download o attacchi basati su USB

3. Obiettivi

3.1 Proteggere l'integrità, la disponibilità e la riservatezza dei sistemi endpoint e dei dati da essi trattati mediante misure affidabili di prevenzione, rilevamento e risposta al malware.

3.2 Prevenire l'esecuzione o la propagazione di codice malevolo sulle reti dell'organizzazione applicando misure di sicurezza tecniche, configurazioni di base sicure e telemetria in tempo reale.

3.3 Integrare la protezione degli endpoint con gli altri controlli del SGSI, inclusi la gestione delle vulnerabilità, il controllo degli accessi, la registrazione e il monitoraggio e la risposta agli incidenti.

3.4 Garantire una visibilità continua sugli endpoint tramite piattaforme di protezione gestite centralmente, inclusi agenti antivirus/antimalware, Endpoint Detection and Response (EDR) e telemetria SIEM.

3.5 Assicurare la conformità ai requisiti legali, normativi e basati su standard che impongono la sicurezza degli endpoint, ad esempio l'articolo 32 del GDPR, l'articolo 21 della NIS2 e l'articolo 9 del DORA.

3.6 Definire ruoli con responsabilità chiare, applicare SLA per la gestione delle patch e degli avvisi e garantire la capacità di dimostrare la conformità mediante documentazione e reportistica.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO)

4.1.1 È il titolare della politica e ne assicura l'allineamento con il SGSI e con la strategia complessiva di sicurezza.

4.1.2 Riesamina trimestralmente le metriche di protezione degli endpoint, le tendenze degli incidenti e l'efficacia degli strumenti.

4.1.3 Approva le eccezioni e le accettazioni del rischio residuo relative alla copertura degli endpoint.

4.2 Responsabile della sicurezza degli endpoint / Responsabile del SOC

4.2.1 Gestisce i sistemi di protezione degli endpoint, ad esempio AV, EDR e MDM.

4.2.2 Supervisiona l'applicazione della politica, la taratura del rilevamento delle minacce e i playbook di risposta.

4.2.3 Mantiene le statistiche di copertura, i log degli incidenti malware e le configurazioni di base degli avvisi.

[... 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 annualmente o quando:

9.1.1 si verificano campagne malware rilevanti o incidenti di sicurezza degli endpoint

9.1.2 nuovi tipi di minaccia, ad esempio malware fileless o varianti ransomware, richiedono strategie aggiornate di rilevamento o risposta

9.1.3 le piattaforme di protezione degli endpoint o le architetture degli agenti cambiano in modo significativo

9.1.4 vengono aggiornati requisiti legali o normativi che incidono sui controlli degli endpoint

9.2 Il riesame deve essere avviato dal Responsabile della sicurezza degli endpoint e coordinato con il CISO e con le funzioni Legale, Risk Management e Internal Audit.

9.3 Le revisioni approvate devono essere documentate nel registro di controllo documentale del SGSI, deve essere assegnato un nuovo identificativo di versione e la comunicazione deve essere trasmessa a tutte le parti interessate.

9.4 Le versioni superate devono essere archiviate con accesso limitato e conservate ai fini dell'integrità della traccia di audit, in conformità con i piani di conservazione del SGSI.

10. Politiche correlate e collegamenti

10.1 P1 - Politica per la sicurezza delle informazioni. Stabilisce i principi fondamentali per la protezione di sistemi, dati e reti. La presente politica applica tali principi a livello di endpoint attraverso controlli tecnici e procedurali contro il malware.

10.2 P4 - Politica di controllo degli accessi. Definisce le restrizioni di accesso degli utenti applicate a livello di endpoint, incluse le protezioni contro l'elevazione dei privilegi e le installazioni non autorizzate di software non verificato.

10.3 P5 - Politica di gestione delle modifiche. Assicura che gli aggiornamenti al software di protezione degli endpoint, alle regole di policy o alle configurazioni degli agenti siano soggetti a processi approvativi e di rilascio controllato.

10.4 P12 - Politica di gestione degli asset. Fornisce la baseline di classificazione e inventario degli asset necessaria per la visibilità sugli endpoint, la copertura delle patch e la definizione dell'ambito della protezione dal malware.

10.5 P22 - Politica di logging e monitoraggio. Consente l'integrazione degli avvisi degli endpoint, dello stato di salute degli agenti e delle informazioni sulle minacce nei sistemi SIEM centralizzati per il rilevamento in tempo reale e la tracciabilità forense.

10.6 P30 - Politica di risposta agli incidenti (P30). Collega gli incidenti malware sugli endpoint a workflow standardizzati di contenimento, eradicazione, indagine e ripristino con ruoli assegnati e soglie di escalation.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001:

11.1.1 Clausola 8.1 - Pianificazione e controllo operativi: richiede l'implementazione di controlli tecnici, incluse misure di protezione degli endpoint, per mantenere gli obiettivi del SGSI.

11.2 ISO/IEC 27002:2022 - Controlli 8.7, 8:

11.2.1 Fornisce linee guida tecniche dettagliate sulle misure antimalware, sul rilascio sicuro del software, sul monitoraggio e sulla preparazione agli incidenti per gli ambienti endpoint.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Protezione dal codice malevolo: richiede l'uso di strumenti antimalware con scansione in tempo reale, scansione all'accesso e analisi comportamentale.

11.3.2 SI-4 - Monitoraggio dei sistemi: supporta l'integrazione della telemetria con piattaforme di rilevamento centralizzate.

11.3.3 CM-6 - Impostazioni di configurazione: rafforza le impostazioni di controllo della configurazione di base sugli endpoint, inclusa l'applicazione degli agenti di protezione.

11.4 Regolamento generale sulla protezione dei dati (GDPR) UE (2016/679):

11.4.1 Articolo 32 - Sicurezza del trattamento: richiede alle organizzazioni di implementare misure tecniche adeguate per tutelare i dati personali, inclusa la protezione contro le minacce malware.

11.5 Direttiva UE NIS2 (2022/2555):

11.5.1 Articolo 21(2)(d): obbliga i soggetti a implementare misure di rilevamento e prevenzione delle minacce, inclusi meccanismi di difesa dal malware a livello di endpoint.

11.6 Regolamento UE DORA (2022/2554):

11.6.1 Articolo 9 - Requisiti di gestione del rischio ICT: richiede che le entità finanziarie adottino misure di protezione per prevenire, rilevare e rispondere al malware e alle minacce veicolate tramite endpoint.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Protect Against Malware: richiede il rilevamento e la mitigazione del malware su tutti gli endpoint dell'organizzazione.

11.7.2 DSS01.04 - Manage Availability and Capacity: assicura che la protezione dal malware sia bilanciata con le prestazioni del sistema e la continuità operativa.

11.7.3 MEA03 - Monitor, Evaluate and Assess Compliance: richiede audit periodici dei controlli sugli endpoint e dell'efficacia della protezione.