					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P19					Titolo del documento: **Politica di gestione delle vulnerabilità e delle patch**							
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

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Trattamento sistematico delle vulnerabilità tecniche; efficacia continuativa dei controlli di sicurezza.
ISO/IEC 27002:2022	Controlli 8.8, 8.9, 5	Linee guida di attuazione per l'applicazione delle patch, le scansioni di vulnerabilità, l'integrità del software, la configurazione sicura e l'inventario degli asset.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Scansioni frequenti, rimedio delle vulnerabilità e gestione della configurazione applicati.
GDPR UE	Articolo 32, Considerando 49	Misure tecniche per la tempestiva applicazione delle patch, il trattamento delle vulnerabilità e la continuità della sicurezza.
NIS2 UE	Articolo 21(2)(d)	Rilevazione, risposta e mitigazione delle vulnerabilità per un elevato livello di igiene informatica.
DORA UE	Articoli 8, 10(2)(f)	Rimedio tempestivo delle vulnerabilità ICT; valutazioni continue delle minacce basate su scenari di minaccia.
COBIT 2019	DSS05.02, DSS01.03, MEA	Scansionare, tracciare e mitigare le debolezze tecniche; monitorare lo sfruttamento; verificare mediante audit l'efficacia, incluso lo stato delle patch.

1. Finalità

1.1 La presente politica definisce i requisiti obbligatori dell'organizzazione per identificare, classificare, correggere e monitorare le vulnerabilità tecniche e i difetti software in tutti i sistemi informativi e gli asset compresi nel campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

1.2 Essa assicura che tutte le vulnerabilità note siano valutate e trattate tempestivamente e in base al rischio, mediante l'applicazione coordinata di patch, adeguamenti di configurazione o controlli compensativi, in coerenza con le esigenze aziendali e gli obblighi di conformità.

1.3 La presente politica supporta la conformità al controllo 8.8 dell'Allegato A della ISO/IEC 27001 e alle linee guida della ISO/IEC 27002, e recepisce i requisiti normativi di cui all'articolo 8 del DORA, all'articolo 21 della NIS2, all'articolo 32 del GDPR e ai domini DSS e APO di COBIT 2019.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i sistemi informativi, gli asset e gli ambienti che archiviano, trattano o trasmettono dati soggetti alla governance del SGSI, inclusi:

2.1.1 Sistemi operativi, applicazioni, dispositivi di rete, firmware, piattaforme cloud, API e software di terze parti.

2.1.2 Sistemi negli ambienti di sviluppo, staging, produzione, backup e disaster recovery.

2.1.3 Endpoint, server, dispositivi IoT, infrastrutture di virtualizzazione e container.

2.2 È vincolante per:

2.2.1 Personale interno: amministratori IT, sistemisti, sviluppatori applicativi, analisti di sicurezza e team infrastrutturali.

2.2.2 Parti esterne: appaltatori e fornitori terzi di servizi, fornitori di servizi gestiti (MSP), fornitori software e integratori di sistema con responsabilità tecniche sugli asset compresi nell'ambito di applicazione.

2.3 La politica copre l'intero ciclo di vita della gestione delle vulnerabilità e delle patch, inclusi:

2.3.1 Scansione e rilevazione

2.3.2 Classificazione del rischio e prioritizzazione

2.3.3 Acquisizione, test, distribuzione e rollback delle patch

2.3.4 Gestione delle eccezioni e pianificazione dei controlli compensativi

2.3.5 Registrazione, reportistica e tracciabilità ai fini di audit

3. Obiettivi

3.1 Assicurare che tutte le vulnerabilità note siano identificate, valutate e corrette in modo da ridurre al minimo l'esposizione residua e allinearsi alle priorità operative.

3.2 Stabilire processi coerenti a livello aziendale per le scansioni di vulnerabilità, la classificazione della gravità (ad es. CVSS) e la gestione delle patch, inclusa la gestione delle emergenze e la pianificazione del rollback.

3.3 Consentire una gestione sicura della configurazione mediante allineamento con le baseline di hardening, le pratiche di gestione delle modifiche e le informazioni sulle minacce in tempo reale.

3.4 Fornire una conformità misurabile ai controlli normativi e agli standard relativi all'integrità dei sistemi, all'igiene delle patch e al tempestivo rimedio dei difetti.

3.5 Definire responsabilità e accountability tra i ruoli per l'intero ciclo di vita della gestione delle vulnerabilità, assicurando che tutte le parti interessate operino entro gli SLA definiti e nel rispetto delle metriche di controllo oggetto di reportistica.

3.6 Rafforzare la preparazione agli audit e migliorare la resilienza rispetto ai rischi emergenti, incluse vulnerabilità zero-day, catene di exploit attive e comunicazioni dei fornitori ad alta rilevanza.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO)

4.1.1 È il titolare della politica e ne assicura l'integrazione nel SGSI.

4.1.2 Definisce la propensione al rischio aziendale e ne assicura l'allineamento con i requisiti normativi e di controllo.

4.2 Responsabile della gestione delle vulnerabilità / Responsabile delle operazioni di sicurezza

4.2.1 Supervisiona le attività end-to-end di gestione delle vulnerabilità e delle patch.

4.2.2 Coordina la pianificazione delle scansioni, i modelli di prioritizzazione e le tempistiche di rimedio.

4.2.3 Mantiene il registro delle vulnerabilità e collabora alla valutazione dei controlli compensativi.

[... 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 o al verificarsi di uno dei seguenti eventi:

9.1.1 aggiornamenti normativi significativi (ad es. modifiche a DORA, NIS2)

9.1.2 cambiamenti nei criteri di prioritizzazione delle vulnerabilità (ad es. aggiornamenti CVSS)

9.1.3 modifiche rilevanti dell'ambiente IT (ad es. migrazione al cloud, revisione sostanziale dell'EDR)

9.1.4 incidenti ad alta rilevanza o avvisi esterni che richiedano un rafforzamento della politica

9.2 I riesami devono essere condotti dal CISO in collaborazione con le operazioni di sicurezza, la gestione del rischio per la sicurezza delle informazioni e la direzione infrastrutturale.

9.3 Gli aggiornamenti della politica devono essere:

9.3.1 documentati nel registro di controllo documentale del SGSI

9.3.2 riesaminati e approvati dalla direzione esecutiva

9.3.3 comunicati a tutte le parti interessate coinvolte, inclusi i responsabili del trattamento terzi

9.4 Le versioni storiche devono essere conservate in modo sicuro per finalità di audit e accountability.

10. Politiche correlate e collegamenti

10.1 P1 - Politica per la sicurezza delle informazioni. Definisce l'impegno generale a proteggere sistemi e dati, inclusa la gestione proattiva delle vulnerabilità e la garanzia dell'integrità del software.

10.2 P5 - Politica di gestione delle modifiche. Disciplina tutte le distribuzioni delle patch e gli adeguamenti di configurazione, richiedendo documentazione, test, approvazione e procedure di rollback che integrano i processi di rimedio delle vulnerabilità.

10.3 P6 - Politica di gestione del rischio. Supporta la classificazione e il trattamento delle vulnerabilità non corrette mediante valutazioni del rischio strutturate, analisi di impatto e procedure di accettazione del rischio residuo.

10.4 P12 - Politica di gestione degli asset. Assicura che i sistemi siano inventariati e classificati correttamente, consentendo scansioni di vulnerabilità coerenti, assegnazione della titolarità e copertura delle patch lungo il ciclo di vita.

10.5 P22 - Politica di registrazione e monitoraggio. Definisce i requisiti per la rilevazione degli eventi e la generazione della traccia di audit. La presente politica supporta la visibilità sulle attività di applicazione delle patch, sulle modifiche non autorizzate e sui tentativi di exploit che prendono di mira vulnerabilità note.

10.6 P30 - Politica di risposta agli incidenti (P30). Specifica i protocolli di escalation e le strategie di contenimento per le vulnerabilità sfruttate, le indagini sulle violazioni e le azioni correttive in linea con i controlli della presente politica.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001: Clausola 8.1 - Pianificazione e controllo operativo: richiede il trattamento sistematico delle vulnerabilità tecniche per garantire l'efficacia continuativa dei controlli di sicurezza.

11.2 ISO/IEC 27002:2022 - Controlli 8.8, 8.9, 5: fornisce linee guida di attuazione per l'applicazione delle patch, le scansioni di vulnerabilità, l'integrità del software e l'integrazione con la configurazione sicura e l'inventario degli asset.

11.3 NIST SP 800-53 Rev.5: RA-5 - Monitoraggio e scansione delle vulnerabilità: impone scansioni frequenti e il tracciamento delle attività di rimedio. SI-2 - Rimedio dei difetti: richiede la valutazione tempestiva e la mitigazione dei difetti mediante patch disponibili o altre azioni. CM-2 / CM-6 - Baseline e controlli di gestione della configurazione: stabilisce le basi per configurazioni di sistema sicure collegate all'applicazione delle patch.

11.4 GDPR UE (2016/679): Articolo 32 - Sicurezza del trattamento: richiede l'implementazione di misure tecniche adeguate, quali la tempestiva applicazione delle patch e il trattamento delle vulnerabilità, per garantire la riservatezza e la resilienza dei sistemi. Considerando 49: incoraggia i

soggetti ad attuare controlli preventivi contro minacce note a supporto della sicurezza e della continuità operativa.

11.5 Direttiva UE NIS2 (2022/2555): Articolo 21(2)(d): obbliga i soggetti essenziali e importanti a rilevare, rispondere e mitigare le vulnerabilità dei sistemi e a mantenere un elevato livello di igiene informatica.

11.6 DORA UE (2022/2554): Articolo 8 - Gestione del rischio ICT: richiede l'identificazione e il tempestivo rimedio delle vulnerabilità nelle tecnologie dell'informazione e della comunicazione utilizzate nei sistemi finanziari. Articolo 10(2)(f): enfatizza valutazioni continue delle vulnerabilità guidate dalle minacce e l'applicazione delle patch come parte della resilienza operativa.

11.7 COBIT 2019: DSS05.02 - Gestire le vulnerabilità di sicurezza: indirizza le organizzazioni a scansionare, tracciare e mitigare le debolezze tecniche note. DSS01.03 - Monitorare l'infrastruttura: assicura che i sistemi siano monitorati per rilevare segni di sfruttamento o debolezza. MEA03 - Monitor, Evaluate, and Assess Compliance: richiede audit regolari sull'efficacia dei controlli, incluso lo stato delle patch e la gestione delle eccezioni.