					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P18					Titolo del documento: **Politica sui controlli crittografici**							
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	-
ISO/IEC 27002:2022	Controlli 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12 to SC-17, SC-28, SC-28(1), SC-12(3)	-
GDPR UE	Articolo 32, Articoli 33–34, Considerando 83	-
NIS2 UE	Articolo 21(2)(d)	-
DORA UE	Articoli 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Finalità

1.1 La presente politica definisce i requisiti obbligatori per l'uso sicuro e conforme dei controlli crittografici in tutta l'organizzazione, al fine di garantire la riservatezza, l'integrità e l'autenticità delle informazioni sensibili e soggette a regolamentazione.

1.2 L'uso della crittografia costituisce un elemento fondamentale per la fiducia nelle operazioni di sicurezza dei dati, supporta le comunicazioni sicure, rafforza il controllo degli accessi e consente la conformità normativa attraverso efficaci pratiche di cifratura e gestione delle chiavi.

1.3 La presente politica è allineata alla Clausola 8.1 della ISO/IEC 27001:2022 e al Controllo 8.24 dell'Allegato A, e supporta gli obblighi legali e operativi ai sensi dell'Articolo 32 del GDPR, dell'Articolo 6(2)(d) del DORA e dell'Articolo 21 della NIS2. Supporta inoltre gli obiettivi del COBIT 2019 relativi ai servizi di sicurezza e alla protezione degli asset informativi.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le unità organizzative, alle funzioni aziendali, al personale e ai fornitori terzi coinvolti nell'uso, nell'amministrazione o nell'applicazione di strumenti e metodi crittografici.

2.2 Gli ambienti coperti includono i sistemi di produzione, sviluppo, collaudo, backup e disaster recovery nei quali i dati sensibili sono trasmessi, trattati o archiviati.

2.3 L'ambito di applicazione comprende tutti i componenti crittografici e i relativi casi d'uso, inclusi, a titolo esemplificativo e non esaustivo:

2.3.1 Cifratura simmetrica e asimmetrica

2.3.2 Firme digitali e certificati

2.3.3 Algoritmi di hash

2.3.4 Generazione, distribuzione e distruzione sicure delle chiavi

2.3.5 Transport Layer Security (TLS), cifratura completa del disco (FDE) e cifratura a livello di API

2.3.6 Componenti sicuri quali Hardware Security Module (HSM), Trusted Platform Module (TPM) e Key Management System (KMS)

2.4 La presente politica disciplina l'uso della crittografia in relazione a:

2.4.1 Dati classificati come Riservati, Altamente riservati o Regolamentati

2.4.2 Autenticazione e verifica dell'identità digitale

2.4.3 Comunicazioni sicure con soggetti esterni

2.4.4 Custodia delle chiavi e meccanismi di doppio controllo

3. Obiettivi

3.1 Garantire che le tecnologie crittografiche siano selezionate, approvate, applicate e mantenute in conformità al rischio aziendale, agli standard internazionali e ai requisiti normativi.

3.2 Stabilire una struttura di governance standardizzata per la gestione dei servizi crittografici, incluse responsabilità chiaramente definite in materia di applicazione, convalida e gestione delle eccezioni.

3.3 Prevenire l'uso non autorizzato, la configurazione errata o l'obsolescenza di algoritmi e controlli crittografici attraverso un processo formale di approvazione e riesame.

3.4 Garantire che i controlli crittografici siano integrati nella progettazione dei sistemi e convalidati regolarmente per prevenire esposizione dei dati, compromissione delle chiavi o indebolimento dei protocolli.

3.5 Applicare la gestione del ciclo di vita di tutte le chiavi crittografiche, inclusi generazione, archiviazione, utilizzo, rotazione, revoca e distruzione sicura.

3.6 Garantire la conformità ai regolamenti internazionali e regionali che impongono la cifratura e il trattamento sicuro dei dati, inclusi GDPR, DORA, NIS2 e COBIT 2019.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO) / Information Security Manager

4.1.1 È il titolare della politica e ne garantisce l'allineamento con il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e con il Controllo 8.24 dell'Allegato A della ISO/IEC 27001.

4.1.2 Approva l'uso di algoritmi e controlli crittografici e ne garantisce la conformità in tutta l'organizzazione.

4.2 Responsabile operativo della crittografia / Security Architect

4.2.1 Gestisce le operazioni quotidiane e l'amministrazione dei sistemi crittografici.

4.2.2 Mantiene l'elenco dei metodi crittografici approvati (ACML) e il registro di gestione delle chiavi.

4.2.3 Conduce i riesami della progettazione crittografica (CDR) e valuta le nuove tecnologie crittografiche.

[... 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 dall'Information Security Manager e dal Responsabile operativo della crittografia.

9.2 I trigger di riesame includono:

9.2.1 Individuazione di vulnerabilità crittografiche (ad esempio downgrade degli algoritmi, attacchi quantistici)

9.2.2 Modifiche normative che richiedono standard di cifratura aggiornati

9.2.3 Risultanze operative o di audit che evidenziano lacune della politica

9.2.4 Aggiornamenti degli strumenti crittografici o modifiche architetturali

9.3 Gli aggiornamenti devono essere soggetti a controllo di versione nel Registro di controllo documentale del SGSI e comunicati a:

9.3.1 Tutti gli amministratori con ruoli di accesso crittografico

9.3.2 Team di sviluppo e referenti DevSecOps

9.3.3 Fornitori terzi soggetti a obblighi contrattuali di cifratura

9.4 Il team SGSI deve garantire che le versioni superate siano archiviate e non siano più richiamate nelle procedure operative.

10. Politiche correlate e collegamenti

10.1 P1 - Politica per la sicurezza delle informazioni. Fornisce la governance di base per tutte le misure di sicurezza, inclusa l'applicazione dei controlli crittografici, la protezione degli asset e le comunicazioni sicure.

10.2 P4 - Politica di controllo degli accessi. Garantisce che l'accesso logico al materiale crittografico e ai sistemi di gestione della cifratura sia rigorosamente limitato in base al principio del privilegio minimo e alla separazione dei compiti.

10.3 P6 - Politica di gestione del rischio. Supporta la valutazione dei rischi relativi ai controlli crittografici e documenta la strategia di trattamento del rischio per eccezioni, obsolescenza degli algoritmi o scenari di compromissione delle chiavi.

10.4 P12 - Politica di gestione degli asset. Impone la classificazione dei dati sensibili e degli asset hardware, che determina direttamente i requisiti crittografici e gli obblighi di custodia delle chiavi.

10.5 P13 - Politica di classificazione ed etichettatura dei dati. Definisce i livelli di classificazione (ad esempio Riservato, Regolamentato) che attivano specifici requisiti di cifratura in transito e a riposo.

10.6 P14 - Politica di conservazione e smaltimento dei dati. Specifica le procedure per lo smaltimento sicuro dei supporti di archiviazione cifrati e del materiale crittografico a fine vita.

10.7 P30 - Politica di risposta agli incidenti (P30). Definisce la strategia di risposta dell'organizzazione in caso di compromissione delle chiavi, uso improprio dei certificati o sospette vulnerabilità algoritmiche, inclusi revoca rapida e obblighi di notifica della violazione.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 - Pianificazione e controllo operativi: impone controlli tecnici di sicurezza, incluse misure crittografiche, come parte delle misure di protezione operative.

11.2 ISO/IEC 27002:2022

11.2.1 Controlli 8.24, 8.25, 8: fornisce indicazioni applicative sugli obiettivi dei controlli crittografici, sulla selezione degli algoritmi, sull'applicazione dei protocolli e sulla gestione del ciclo di vita dei certificati.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-12 - Definizione delle chiavi crittografiche: garantisce la generazione e lo scambio sicuri delle chiavi di cifratura. La P18 definisce come le chiavi simmetriche e asimmetriche devono essere generate e scambiate utilizzando algoritmi e protocolli approvati.

11.3.2 SC-13 - Protezione crittografica: impone l'uso della crittografia per proteggere la riservatezza e l'integrità delle informazioni. La P18 applica la cifratura dei dati a riposo e in transito in base alla classificazione dei dati, con standard algoritmici allineati al NIST FIPS 140-3.

11.3.3 SC-17 - Certificati dell'Infrastruttura a chiave pubblica (PKI): richiede l'implementazione della PKI a supporto dell'autenticazione e delle firme digitali. La P18 definisce l'uso della PKI per proteggere comunicazioni, identità di sistema e accessi amministrativi.

11.3.4 SC-28, SC-28(1) - Protezione delle informazioni a riposo e in transito: richiede la cifratura dei dati quando sono archiviati o trasmessi su reti non attendibili. La P18 specifica l'applicazione di TLS, tunnel VPN, cifratura completa del disco e metodi di archiviazione sicuri per i dati sensibili.

11.3.5 SC-12(3) - Generazione di chiavi simmetriche per archiviazione e distribuzione sicure: si concentra sulla generazione e gestione sicure delle chiavi simmetriche. La P18 impone l'uso di

generatori di numeri casuali robusti, politiche di rotazione delle chiavi e vault sicuri delle chiavi per le operazioni crittografiche.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 32 - Sicurezza del trattamento: raccomanda espressamente la cifratura come misura di riduzione del rischio per i dati personali.

11.4.2 Considerando 83: sottolinea la cifratura come controllo per prevenire l'accesso non autorizzato ai dati.

11.4.3 Articoli 33 e 34: la cifratura può esonerare le organizzazioni dagli obblighi di notifica della violazione se efficace.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articolo 21(2)(d): richiede misure tecniche e organizzative, incluse protezioni crittografiche, per mantenere disponibilità e integrità dei servizi.

11.6 DORA UE (2022/2554)

11.6.1 Articolo 6(2)(d): gli enti finanziari devono proteggere i dati, anche mediante cifratura forte delle informazioni critiche.

11.6.2 Articolo 11(1)(c): impone controlli sicuri del trattamento dei dati per i fornitori terzi di servizi ICT.

11.7 COBIT 2019

11.7.1 DSS05.01 - Proteggere gli asset informativi: richiede l'uso della cifratura e della gestione delle chiavi per proteggere i dati dall'accesso non autorizzato.

11.7.2 DSS06.06 - Managed Security Testing: raccomanda la convalida della conformità crittografica come parte delle valutazioni di vulnerabilità.

11.7.3 MEA03 - Monitor, Evaluate and Assess Compliance: impone un presidio continuo dell'efficacia dei controlli crittografici.