					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P23					Titolo del documento: **Politica di sincronizzazione dell'orario**							
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	Controllo 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
GDPR UE	Articolo 32	-
NIS2 UE	Articolo 21(2)(e)	-
DORA UE	Articoli 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Finalità

1.1 La presente politica ha lo scopo di garantire che tutti i sistemi, le applicazioni, i dispositivi e i servizi cloud dell'organizzazione mantengano impostazioni temporali coerenti e accurate mediante la sincronizzazione con fonti temporali designate e affidabili.

1.2 Una sincronizzazione accurata dell'orario è essenziale per garantire registrazioni di audit affidabili, comunicazioni sicure, tracciabilità degli audit, risposta agli incidenti e indagini forensi. Il disallineamento temporale può determinare log non correlabili, errori di autenticazione e segnalazioni normative incomplete.

1.3 La presente politica supporta il Controllo 8.17 dell'Allegato A della ISO/IEC 27001 e gli standard internazionali correlati, imponendo l'accuratezza temporale e il rilevamento della deriva dell'orologio nell'intero panorama degli asset IT dell'organizzazione.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutti i componenti dell'infrastruttura, inclusi server, workstation, dispositivi di rete, firewall e sistemi Internet of Things (IoT)

2.1.2 Ambienti virtuali e cloud (ad es. AWS, Azure, Google Cloud)

2.1.3 Tutti i sistemi che partecipano alla registrazione di audit, all'autenticazione, all'elaborazione delle transazioni o alla correlazione degli eventi di sicurezza

2.1.4 Dipendenti interni, collaboratori esterni e fornitori terzi con responsabilità su sistemi sensibili al fattore tempo

2.2 Rientrano nell'ambito di applicazione anche i sistemi che generano o utilizzano registrazioni con marcatura temporale, quali voci di log, allerte, registrazioni delle attività degli utenti o evidenze forensi.

3. Obiettivi

3.1 Definire un'architettura di sincronizzazione dell'orario coerente e centralizzata, utilizzando fonti NTP approvate o equivalenti.

3.2 Garantire che tutti i sistemi sincronizzino i propri orologi a intervalli definiti e che qualsiasi deriva sia rilevata e corretta automaticamente o con intervento minimo.

3.3 Mantenere l'accuratezza dell'orario negli ambienti ibridi, on-premise e cloud per consentire:

3.3.1 Una correlazione affidabile degli eventi e la risposta agli incidenti

3.3.2 La conformità a standard e requisiti normativi quali ISO 27001, GDPR, NIS2 e DORA

3.3.3 La protezione contro gli attacchi di replay e i malfunzionamenti dell'autenticazione basati sul tempo

3.4 Stabilire ruoli chiari, procedure per la gestione delle eccezioni e meccanismi di audit per garantire l'attuazione della politica.

3.5 Garantire che le anomalie temporali siano registrate, generino allerte e siano sottoposte a escalation quando superano le tolleranze definite.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO)

4.1.1 È il proprietario della presente politica e ne garantisce l'allineamento con i controlli operativi del SGSI e con i requisiti normativi.

4.1.2 Approva la selezione delle fonti temporali aziendali e convalida i processi di reporting della sincronizzazione dell'orario.

4.2 Responsabile dei servizi infrastrutturali / Responsabile tecnico dell'ingegneria di rete

4.2.1 Mantiene i server NTP primari e secondari dell'organizzazione o la configurazione della fonte temporale designata.

4.2.2 Garantisce che tutti i dispositivi connessi alla rete e le istanze virtuali sincronizzino l'orario a intervalli appropriati.

4.2.3 Monitora i log di sincronizzazione dell'orario, le allerte di deriva dell'orologio e le condizioni di errore.

[... 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 prima al verificarsi delle seguenti condizioni:

9.1.1 Rilevazione di exploit basati sul tempo o di guasti nella registrazione

9.1.2 Modifiche all'infrastruttura temporale principale (ad es. nuovi server NTP aziendali o aggiornamenti dei protocolli)

9.1.3 Discrepanze nella deriva temporale della piattaforma cloud o modifiche ai servizi regionali

9.1.4 Risultanze post-incidente che identifichino il disallineamento temporale come fattore contribuente

9.2 Il riesame deve essere coordinato dal Responsabile dei servizi infrastrutturali, con il contributo del SOC, della sicurezza applicativa e delle parti interessate della conformità.

9.3 Le revisioni devono essere documentate nel Registro dei documenti del SGSI e comunicate alle parti interessate interne e ai terzi coinvolti.

9.4 Le versioni storiche della politica devono essere archiviate in modo sicuro, sottoposte a controllo di versione e rese disponibili in caso di richieste di audit di conformità o di verifiche legali.

10. Politiche correlate e collegamenti

10.1 P1 – Politica per la sicurezza delle informazioni. Stabilisce il mandato generale per garantire l'integrità e la tracciabilità di tutti i sistemi informativi, per i quali l'accuratezza temporale costituisce un presupposto fondamentale.

10.2 P5 – Politica di gestione delle modifiche. Disciplina le modifiche alle configurazioni di sistema, inclusi gli adeguamenti delle fonti temporali, garantendo adeguata documentazione, test e piani di back-out.

10.3 P22 – Politica di registrazione e monitoraggio. Dipende direttamente dalla sincronizzazione dell'orario per garantire la sequenzialità degli eventi, la correlazione dei log e l'integrità delle indagini sugli incidenti in sistemi eterogenei.

10.4 P30 – Politica di risposta agli incidenti (P30). Si basa su marcature temporali accurate per le indagini forensi, le cronologie degli incidenti e le evidenze della catena di custodia. Un orario non accurato compromette l'attendibilità delle relazioni sugli incidenti.

10.5 P20 – Politica di protezione degli endpoint / Politica antimalware. Richiede allerte temporalmente accurate e analisi comportamentali per rilevare la diffusione di malware, il movimento laterale e le anomalie di accesso.

10.6 P6 – Politica di gestione del rischio. Definisce il trattamento della desincronizzazione come potenziale rischio operativo e forense, richiedendo i controlli definiti nella presente politica per mitigarne l'impatto.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Pianificazione e controllo operativi: richiede l'integrazione di controlli tecnici accurati, quali gli orologi di sistema sincronizzati, per un'esecuzione operativa affidabile.

11.2 ISO/IEC 27002:2022 – Controllo 8

11.2.1 Rafforza l'accuratezza dell'orologio e richiede la coerenza organizzativa dell'orario di sistema per agevolare il confronto dei log, le indagini e la convalida sicura delle transazioni.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Sincronizzazione dell'orario di sistema: richiede la sincronizzazione dell'orario mediante fonti autorevoli in tutti i componenti compresi nel perimetro del sistema.

11.3.2 AU-8 – Marcature temporali: garantisce che gli eventi siano marcati temporalmente in modo accurato e assicura la tracciabilità ai fini dell'audit e della risposta agli incidenti.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 32 – Sicurezza del trattamento: pur non citando esplicitamente il tempo, richiede l'adozione di misure tecniche adeguate, incluse tracce di audit e log, la cui validità e integrità dipendono intrinsecamente da marcature temporali sincronizzate.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articolo 21(2)(e): richiede capacità di registrazione e rilevazione che presuppongono una sincronizzazione accurata dell'orario per la correlazione tra sistemi e una risposta tempestiva.

11.6 DORA UE (2022/2554)

11.6.1 Articolo 9 – Gestione del rischio ICT: richiede telemetria accurata dei sistemi per il monitoraggio del rischio e il rilevamento delle anomalie, che dipendono da una precisa sincronizzazione dell'orologio.

11.6.2 Articolo 10 – Continuità operativa ICT: impone controlli che garantiscano l'integrità dei sistemi durante le interruzioni, incluse registrazioni degli eventi temporalmente allineate.

11.7 COBIT 2019

11.7.1 DSS05.04 – Monitorare gli eventi di sicurezza: richiede l'integrità delle marcature temporali per un'analisi efficace dei log e il rilevamento delle minacce.

11.7.2 MEA03 – Monitor, Evaluate, and Assess Compliance: la sincronizzazione dell'orario supporta audit di conformità accurati e cicli di reporting affidabili.