					Insira aqui a designação da entidade jurídica registada							
Número do documento: P23					Título do documento: **Política de Sincronização Temporal**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	-
ISO/IEC 27002:2022	Controlo 8	-
NIST SP 800-53 Rev. 5	SC-45, AU-8	-
RGPD da UE	Artigo 32	-
Diretiva NIS2 da UE	Artigo 21(2)(e)	-
DORA da UE	Artigos 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Finalidade

1.1 A finalidade desta política é assegurar que todos os sistemas, aplicações, dispositivos e serviços na nuvem da organização mantêm definições de tempo consistentes e exatas através da sincronização com fontes de tempo designadas e fiáveis.

1.2 A sincronização temporal exata é essencial para registo fiável, comunicações seguras, rastreabilidade de auditoria, resposta a incidentes e investigação forense. O desalinhamento temporal pode resultar em logs sem correlação, falhas de autenticação e reporte regulamentar incompleto.

1.3 Esta política suporta o Controlo 8.17 do Anexo A da ISO/IEC 27001 e outras normas internacionais relacionadas, impondo a exatidão temporal e a deteção de deriva de relógio em todo o parque tecnológico de TI da organização.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os componentes de infraestrutura, incluindo servidores, postos de trabalho, dispositivos de rede, firewalls e sistemas IoT

2.1.2 Ambientes virtuais e na nuvem (por exemplo, AWS, Azure, Google Cloud)

2.1.3 Todos os sistemas que participem em registo, autenticação, processamento de transações ou correlação de eventos de segurança

2.1.4 Colaboradores internos, contratados e prestadores de serviços terceiros com responsabilidade sobre sistemas sensíveis ao tempo

2.2 Estão incluídos no âmbito os sistemas que gerem ou consumam registos com marca temporal, como entradas de log, alertas, registos de atividade de utilizadores ou evidência forense.

3. Objetivos

3.1 Definir uma arquitetura consistente e centralizada de sincronização temporal com recurso a fontes NTP aprovadas ou equivalentes.

3.2 Assegurar que todos os sistemas sincronizam os respetivos relógios em intervalos definidos e que qualquer deriva é detetada e corrigida automaticamente ou com intervenção mínima.

3.3 Manter a exatidão temporal em ambientes híbridos, infraestruturas on-premises e ambientes na nuvem, de modo a permitir:

3.3.1 Correlação fiável de eventos e resposta a incidentes

3.3.2 Cumprimento de normas e regulamentos como a ISO 27001, o RGPD da UE, a Diretiva NIS2 da UE e a DORA da UE

3.3.3 Proteção contra ataques de repetição e falhas de autenticação baseadas no tempo

3.4 Estabelecer papéis claros, procedimentos de tratamento de exceções e mecanismos de auditoria para assegurar a aplicação desta política.

3.5 Assegurar que as anomalias relacionadas com o tempo são registadas, geram alertas e são escaladas quando excedem as tolerâncias definidas.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É o responsável por esta política e assegura o alinhamento com os controlos operacionais do SGSI e os requisitos regulamentares.

4.1.2 Aprova a seleção das fontes de tempo empresariais e valida os processos de reporte da sincronização temporal.

4.2 Responsável pelos Serviços de Infraestrutura / Responsável de Engenharia de Redes

4.2.1 Mantém os servidores NTP primário e secundário da organização ou a configuração da fonte de tempo designada.

4.2.2 Assegura que todos os dispositivos de rede e instâncias virtuais sincronizam a hora em intervalos adequados.

4.2.3 Monitoriza os logs de sincronização temporal, os alertas de deriva de relógio e as condições de falha.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Requisitos de revisão e atualização

9.1 Esta política deve ser revista anualmente, ou antes, nas seguintes condições:

9.1.1 Deteção de explorações baseadas no tempo ou falhas de registo

9.1.2 Alterações à infraestrutura temporal principal (por exemplo, novos servidores NTP empresariais ou atualizações de protocolo)

9.1.3 Discrepâncias de deriva temporal em plataformas cloud ou alterações de serviço por região

9.1.4 Conclusões pós-incidente que identifiquem o desalinhamento temporal como fator contribuinte

9.2 A revisão deve ser coordenada pelo Responsável de Infraestrutura, com contributos obrigatórios do SOC, da Segurança das Aplicações e das partes interessadas de conformidade.

9.3 As revisões devem ser documentadas no Registo de Documentos do SGSI e comunicadas às partes interessadas internas e terceiros afetados.

9.4 As versões históricas da política devem ser arquivadas de forma segura, sujeitas a controlo de versões e disponibilizadas para pedidos de auditoria de conformidade ou auditoria jurídica.

10. Políticas relacionadas e interdependências

10.1 P1 – Política de Segurança da Informação. Estabelece o mandato global para assegurar a integridade e a rastreabilidade de todos os sistemas de informação, para o qual a exatidão temporal é um elemento basilar.

10.2 P5 – Política de Gestão de Alterações. Rege as alterações às configurações dos sistemas, incluindo ajustes às fontes de tempo, assegurando documentação, testes e planos de reversão adequados.

10.3 P22 – Política de Registo e Monitorização. Depende diretamente do tempo sincronizado para assegurar a sequenciação de eventos, a correlação de logs e a integridade da investigação de incidentes em sistemas distintos.

10.4 P30 – Política de Resposta a Incidentes. Depende de marcas temporais exatas para investigações forenses, cronologias de incidentes e evidência da cadeia de custódia. A inexatidão temporal compromete a credibilidade dos relatórios de incidente.

10.5 P20 – Política de Proteção de Endpoints / Malware. Requer alertas temporalmente exatos e análise comportamental para detetar propagação de malware, movimento lateral e anomalias de acesso.

10.6 P6 – Política de Gestão de Riscos. Define a dessincronização como um potencial risco operacional e forense, exigindo os controlos definidos nesta política para mitigar o impacto.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Planeamento e controlo operacional: exige a integração de controlos técnicos exatos, como relógios de sistema sincronizados, para uma execução operacional fiável.

11.2 ISO/IEC 27002:2022 – Controlo 8

11.2.1 Reforça a exatidão dos relógios e exige consistência organizacional da hora dos sistemas para facilitar a comparação de logs, a investigação e a validação segura de transações.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-45 – Sincronização temporal do sistema: exige sincronização temporal com recurso a fontes autoritativas em todos os componentes dentro do perímetro do sistema.

11.3.2 AU-8 – Marcação temporal: assegura que os eventos recebem marcação temporal exata e fornece rastreabilidade para auditoria e resposta a incidentes.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 32 – Segurança do Tratamento: embora não refira explicitamente o tempo, exige a utilização de medidas técnicas adequadas, incluindo trilhos de auditoria e logs, que dependem inerentemente de marcas temporais sincronizadas para validade e integridade.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(e): exige capacidades de registo e deteção que pressupõem sincronização temporal exata para correlação entre sistemas e resposta atempada.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 9 – Gestão do risco das TIC: exige telemetria exata dos sistemas para monitorização de riscos e deteção de anomalias, o que depende de sincronização precisa dos relógios.

11.6.2 Artigo 10 – Continuidade de negócio das TIC: impõe controlos que assegurem a integridade dos sistemas durante perturbações, incluindo registos de eventos temporalmente alinhados.

11.7 COBIT 2019

11.7.1 DSS05.04 – Monitorizar eventos de segurança: exige integridade da marcação temporal para análise eficaz de logs e deteção de ameaças.

11.7.2 MEA03 – Monitorizar, avaliar e analisar a conformidade: a sincronização temporal suporta auditoria de conformidade exata e ciclos de reporte.