					Insira aqui a designação da entidade jurídica registada							
Número do documento: P23S					Título do documento: **Política de sincronização horária P23S**							
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**

Alinhado com normas e regulamentos, quando aplicável

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	Requisitos de controlo aplicáveis
ISO/IEC 27002:2022	Controlo 8	Operação sincronizada dos sistemas
NIST SP 800-53 Rev.5	SC-45, AU-8	NTP de confiança e exatidão dos carimbos temporais dos registos
RGPD da UE	Artigos 5(1)(d), 32	Exatidão, responsabilização e integridade dos dados pessoais com carimbos temporais sincronizados
Diretiva NIS2 da UE	Artigo 21(2)(d)	Capacidades de monitorização/deteção suportadas por registos sincronizados
DORA da UE	Artigos 10, 15	Resiliência operacional e registos técnicos exatos
COBIT 2019	DSS05.02, MEA03	Eventos com carimbo temporal e monitorização baseada em evidências

1. Finalidade

1.1 A presente política estabelece controlos obrigatórios para manter a hora exata e sincronizada em todos os sistemas que armazenam, transmitem ou processam dados da organização.

1.2 A sincronização horária é essencial para assegurar a rastreabilidade dos registos dos sistemas, a correta correlação de incidentes de segurança e a fiabilidade da evidência utilizada em análise forense ou apreciação jurídica.

1.3 A organização impõe a sincronização horária automática como requisito fundamental para a integridade da auditoria, a resposta a incidentes e a conformidade regulamentar ao abrigo da ISO 27001, do RGPD, da DORA e da NIS2.

1.4 A presente política assegura que todos os sistemas utilizam fontes horárias de confiança, impede a alteração manual das definições de hora e exige a correção atempada de desvios do relógio.

2. Âmbito

2.1 A presente política aplica-se a:

2.1.1 Todos os sistemas e dispositivos propriedade da empresa, incluindo servidores, computadores de secretária, computadores portáteis, dispositivos móveis, firewalls, routers e máquinas virtuais

2.1.2 Infraestruturas remotas e alojadas na cloud utilizadas nas operações (por exemplo, AWS, Microsoft 365, plataformas SaaS)

2.1.3 Sistemas que geram ou armazenam registos de eventos, registos de autenticação ou trilhos de auditoria

2.1.4 Qualquer colaborador, prestador de serviços, fornecedor ou prestador de suporte de TI responsável pela configuração ou manutenção destes sistemas

2.2 A política aplica-se igualmente a dispositivos BYOD (Bring Your Own Device) utilizados para aceder a sistemas empresariais, desde que esses dispositivos armazenem ou gerem dados relevantes para auditoria.

3. Objetivos

3.1 Assegurar que todos os sistemas críticos sincronizam automaticamente a hora utilizando servidores Network Time Protocol (NTP) de confiança ou mecanismos equivalentes do fornecedor de cloud

3.2 Prevenir discrepâncias horárias que possam comprometer a fiabilidade ou a correlação dos registos dos sistemas durante auditorias ou investigações de segurança

3.3 Permitir a deteção e correção atempadas de desvios de hora para além dos limiares aceitáveis

3.4 Manter a consistência dos carimbos temporais entre ambientes locais, na cloud e remotos

3.5 Cumprir os requisitos técnicos e legais relativos à integridade, rastreabilidade e não repúdio de registos e eventos

4. Papéis e responsabilidades

4.1 Diretor-Geral (DG)

4.1.1 Aprova a presente política e assegura o respetivo cumprimento na organização

4.1.2 Supervisiona as revisões periódicas da exatidão horária ao nível dos sistemas e das lacunas de implementação

4.1.3 Aprova exceções à sincronização horária automática, quando justificadas e documentadas

4.2 Prestador de suporte de TI / função interna de TI

4.2.1 Configura a sincronização horária em todos os sistemas propriedade da empresa ou por esta geridos

4.2.2 Verifica diariamente ou de acordo com o calendário definido se a sincronização está a funcionar corretamente

4.2.3 Investiga e corrige eventos de desvio horário, falhas de sincronização ou problemas de acesso a NTP

4.2.4 Documenta o estado da sincronização horária no âmbito das verificações mensais do estado dos sistemas

[... 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 Revisão programada

9.1.1 A presente política deve ser revista anualmente pelo Diretor-Geral, pelo prestador de suporte de TI e pelo Coordenador de Privacidade

9.1.2 Todos os registos e relatórios de estado do cumprimento da sincronização horária devem ser considerados durante a revisão

9.2 Atualizações desencadeadas por eventos

9.2.1 A presente política deve ser atualizada se:

9.2.1.1 Uma falha de sistema resultar num desvio horário significativo

9.2.1.2 Uma auditoria revelar deficiências na sincronização horária

9.2.1.3 A organização adotar novos ambientes cloud, híbridos ou de virtualização

9.2.1.4 Alterações legais ou regulamentares introduzirem novos requisitos de integridade horária

9.3 Controlo de versões e comunicação

9.3.1 Todas as atualizações devem estar sujeitas a controlo de versão e ser datadas

9.3.2 As alterações significativas devem ser comunicadas a todo o pessoal técnico

9.3.3 As versões anteriores devem ser conservadas durante 3 anos para suporte à auditoria

10. Políticas relacionadas e ligações

10.1 A presente política deve ser aplicada em conjunto com as seguintes políticas SME:

10.1.1 P22S – Política de registo e monitorização: assegura a consistência dos carimbos temporais nos registos para rastreabilidade e correlação forense.

10.1.2 P30S – Política de resposta a incidentes: depende da exatidão dos carimbos temporais para reconstituir incidentes, definir cronologias e suportar decisões de notificação.

10.1.3 P17S – Política de proteção de dados e privacidade: assegura que os registos de acesso e as cronologias de tratamento de dados que envolvam dados pessoais são exatos e defensáveis ao abrigo do RGPD.

10.1.4 P12S – Política de gestão de ativos: suporta a identificação dos sistemas que requerem sincronização, em particular dispositivos móveis e remotos.

10.1.5 P26S – Política de segurança de terceiros e fornecedores: assegura contratualmente que os fornecedores que acedem a dados da organização ou os registam seguem práticas de sincronização horária.

11. Normas e referenciais

11.1 ISO/IEC 27001:

11.1.1 Cláusula 8.1 – Exige a implementação dos controlos necessários para operações seguras, incluindo registo e aposição de carimbos temporais.

11.2 ISO/IEC 27002:

11.2.1 Controlo 8.17 – Recomenda a sincronização horária para todos os sistemas que produzem registos ou operam de forma colaborativa.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Exige a utilização de fontes horárias internas ou externas para assegurar a exatidão dos carimbos temporais dos registos.

11.3.2 SC-45 – Especifica a utilização de fontes NTP de confiança e a prevenção de alterações manuais da hora em sistemas críticos.

11.4 RGPD da UE:

11.4.1 Artigo 5(1)(d) – Exige exatidão e responsabilização no tratamento de dados pessoais, suportadas por carimbos temporais sincronizados.

11.4.2 Artigo 32 – Exige medidas de segurança que assegurem a integridade dos dados, incluindo períodos de registo consistentes.

11.5 Diretiva NIS2 da UE:

11.5.1 Artigo 21(2)(d) – Exige capacidades de monitorização e deteção, suportadas por registos de sistemas sincronizados.

11.6 DORA da UE:

11.6.1 Artigo 10 – Exige resiliência operacional, requerendo registos de incidentes de TIC rastreáveis e com carimbo temporal.

11.6.2 Artigo 15 – Exige que os prestadores de serviços mantenham registos técnicos exatos, incluindo trilhos de auditoria com carimbo temporal.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Salienta a integridade dos carimbos temporais para detetar e responder a eventos.

11.7.2 MEA03.01 – Exige monitorização do desempenho baseada em evidências, suportada por dados exatos e sincronizados no tempo.