					Insira aqui a designação da entidade jurídica registada							
Número do documento: P22					Título do documento: **Política de Registo e Monitorização**							
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**

1. Finalidade

1.1 A finalidade desta política é estabelecer requisitos claros e aplicáveis para a geração, proteção, revisão e análise de logs que registem eventos críticos de sistema e de segurança em todo o ambiente de TI da organização.

1.2 O registo e a monitorização são essenciais para a deteção de anomalias, a resposta a ameaças, a investigação forense, a demonstração de conformidade em auditoria e o cumprimento de obrigações legais. Esta política assegura que todos os eventos gerados pelos sistemas são devidamente registados, retidos e correlacionados com precisão, através de registos temporalmente sincronizados.

1.3 Esta política é essencial para suportar a Cláusula 8.1 da ISO/IEC 27001 e os Controlos do Anexo A 8.15 (Registo), 8.16 (Monitorização) e 8.17 (Sincronização de Relógios), estando diretamente alinhada com obrigações regulamentares ao abrigo do RGPD da UE, da Diretiva NIS2 da UE, da DORA da UE e do COBIT 2019.

2. Âmbito

2.1 Esta política aplica-se a todos os sistemas, serviços e ambientes que armazenem, tratem ou transmitam dados abrangidos pelo Sistema de Gestão da Segurança da Informação (SGSI), incluindo:

2.1.1 infraestruturas on-premises, serviços alojados na nuvem (por exemplo, IaaS, PaaS, SaaS) e ambientes híbridos

2.1.2 sistemas operativos, bases de dados, aplicações e dispositivos de rede

2.1.3 sistemas de segurança, tais como SIEM, firewalls, plataformas EDR, concentradores VPN e fornecedores de identidade

2.2 Estão abrangidas pelo presente âmbito as seguintes partes interessadas:

2.2.1 utilizadores internos com privilégios de sistema ou administrativos

2.2.2 pessoal de infraestrutura e operações de TI

2.2.3 Centro de Operações de Segurança (SOC) e equipas de deteção de ameaças

2.2.4 programadores de software e proprietários de aplicações

2.2.5 prestadores de serviços terceiros que gerem sistemas que produzem logs

3. Objetivos

3.1 Assegurar que todos os sistemas críticos geram logs de eventos de segurança e registos de atividade do sistema, conservados em conformidade com requisitos regulamentares, legais e contratuais.

3.2 Definir os tipos mínimos de eventos e o conteúdo mínimo dos logs necessários para detetar atividades não autorizadas, rastrear ações de utilizadores e suportar investigações forenses.

3.3 Aplicar medidas de proteção para prevenir a adulteração de logs, a eliminação não autorizada ou o acesso não controlado aos dados de log.

3.4 Estabelecer sistemas centralizados de registo e alerta (por exemplo, SIEM) para agregar, correlacionar e escalar atividade suspeita em tempo quase real.

3.5 Assegurar a sincronização dos relógios dos sistemas, de modo a permitir a correlação precisa entre sistemas e a análise de incidentes.

3.6 Permitir a melhoria contínua e a conformidade através da integração da monitorização de logs com processos de auditoria, risco e gestão de incidentes.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É o responsável por esta política e assegura o seu alinhamento com a postura de risco da organização, os requisitos de auditoria e as obrigações do SGSI.

4.1.2 Aprova o âmbito do registo para sistemas regulados ou de alto risco e supervisiona o reporte de conformidade.

4.2 Gestor do Centro de Operações de Segurança (SOC)

4.2.1 Opera e mantém plataformas centralizadas de gestão de logs (por exemplo, SIEM).

4.2.2 Define regras de agregação de logs, limiares de alerta e vias de escalonamento para triagem de incidentes.

4.2.3 Revê relatórios diários e assegura que as anomalias são analisadas, documentadas e escaladas conforme necessário.

[... 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 antecipadamente, em resposta a:

9.1.1 alterações de impacto material na arquitetura dos sistemas ou na infraestrutura de registo (por exemplo, migração de SIEM)

9.1.2 revisões dos requisitos regulamentares de registo (por exemplo, requisitos de registo ao abrigo da NIS2 ou da DORA)

9.1.3 constatações de auditoria ou análises pós-incidente

9.1.4 ameaças emergentes que exijam monitorização reforçada (por exemplo, ameaças internas, comprometimento da cadeia de abastecimento)

9.2 O processo de revisão deve ser liderado pelo Gestor do Centro de Operações de Segurança (SOC), em coordenação com o CISO, a Gestão de Riscos, a Conformidade e as equipas de Infraestrutura de TI.

9.3 As alterações aprovadas devem ficar sujeitas a controlo de versões no Registo de Controlo Documental do SGSI e ser comunicadas a:

9.3.1 todas as partes interessadas com responsabilidade pela manutenção dos sistemas de registo

9.3.2 proprietários de aplicações e proprietários de sistemas

9.3.3 prestadores de serviços terceiros com responsabilidades de telemetria ou de integração com o SIEM

9.4 Todas as versões substituídas devem ser arquivadas de forma segura, com acesso restrito a responsáveis autorizados do SGSI para efeitos de auditoria e legais.

10. Políticas relacionadas e ligações

10.1 P1 – Política de Segurança da Informação. Estabelece o compromisso fundamental de proteger sistemas e dados, no âmbito do qual o registo e a monitorização funcionam como mecanismos críticos de deteção e resposta.

10.2 P4 – Política de Controlo de Acesso. Assegura que os acessos privilegiados, as autenticações de utilizadores e os eventos de autorização são capturados em logs e monitorizados quanto a abuso ou comportamento anómalo.

10.3 P5 – Política de Gestão de Alterações. Exige o registo de alterações de sistema, implementações de patches e atualizações de configuração que possam introduzir risco ou modificações não autorizadas.

10.4 P21 – Política de Segurança de Rede. Exige registo ao nível da rede (por exemplo, logs de firewall, alertas IDS/IPS, atividade VPN) e integração com o SIEM para visibilidade sobre anomalias de tráfego e proteção de perímetro.

10.5 P23 – Política de Sincronização Temporal. Impõe consistência dos relógios entre sistemas, o que é essencial para um registo fiável e para a correlação de eventos de segurança em múltiplos ambientes.

10.6 P30 – Política de Resposta a Incidentes. Depende dos dados de log e dos mecanismos de alerta para identificar, investigar e responder a incidentes de segurança, preservando também artefactos forenses para revisão pós-incidente.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Planeamento e Controlo Operacional: Exige controlos para monitorizar operações e salvaguardar contra acessos não autorizados e utilização indevida de sistemas.

11.2 ISO/IEC 27002:2022 – Controlos 8.15, 8.16, 8.17

11.2.1 Define requisitos detalhados de registo, incluindo que eventos devem ser registados, como proteger e analisar logs e como assegurar a fiabilidade dos carimbos temporais entre sistemas.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 a AU-12: Abrange seleção de eventos, registo, proteção, revisão de auditoria, resposta a falhas de auditoria e retenção de registos de auditoria.

11.3.2 SI-4 – Monitorização do Sistema: Exige monitorização ativa do sistema com alertas baseados em atividade anómala.

11.3.3 SC-45 – Sincronização Temporal do Sistema: Reforça a exatidão temporal para rastreabilidade de eventos e correlação de incidentes.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 32 – Segurança do Tratamento: Exige controlos técnicos, como registo e monitorização, para assegurar segurança e responsabilização, em particular no acesso a dados pessoais.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(e): Exige sistemas de registo de eventos e monitorização para deteção e resposta rápidas a incidentes de segurança.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 9 – Gestão do Risco das TIC: Exige mecanismos para detetar atividade anómala, registar incidentes e conservar dados forenses.

11.6.2 Artigo 11 – Teste de Planos de Continuidade de Negócio das TIC: Dá ênfase à continuidade da monitorização e à validação da disponibilidade dos logs durante perturbações operacionais.

11.7 COBIT 2019

11.7.1 DSS01.05 – Gerir Logs de Segurança: Exige a implementação de capacidades de registo para toda a infraestrutura crítica.

11.7.2 DSS05.04 – Monitorizar Eventos de Segurança: Exige monitorização e análise em tempo real dos logs para detetar e responder a eventos.

11.7.3 MEA03 – Monitorizar, Avaliar e Analisar a Conformidade: Exige revisão regular das práticas de registo e do alinhamento com os objetivos de controlo.