					Insira aqui a designação da entidade jurídica registada							
Número do documento: P22S					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**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	Controlos operacionais, incluindo registo
ISO/IEC 27002:2022	Controlos 8.15, 8.16, 8.17	Registo de eventos, proteção e monitorização
NIST SP 800-53 Rev.5	AU-2 a AU-12, SI-4	Conteúdo e revisão de registos de auditoria, retenção, deteção de anomalias e alertas
RGPD da UE	Artigos 5(1)(f), 32, 33	Confidencialidade e integridade dos dados, medidas técnicas e notificação de violações
Diretiva NIS2 da UE	Artigos 21(2)(d), 23	Mecanismos de registo para deteção de anomalias e notificação de incidentes no prazo de 24 horas
DORA da UE	Artigos 10, 15	Resiliência operacional, monitorização e registo de prestadores de serviços
COBIT 2019	DSS01.03, DSS05.02	Rastreabilidade da atividade e proteção através de registo e monitorização

1. Finalidade

1.1 A presente política estabelece controlos obrigatórios de registo e monitorização para assegurar a segurança, a responsabilização e a integridade operacional dos sistemas de TI da organização.

1.2 Define os tipos de eventos que devem ser registados, a forma como os registos são armazenados, como são revistos e as responsabilidades dos colaboradores e prestadores de serviços.

1.3 O registo e a monitorização apoiam a deteção de ameaças, o cumprimento regulamentar, a resposta a incidentes e a análise forense.

1.4 Esta política permite à organização cumprir os requisitos de controlo operacional da ISO/IEC 27001 e sustentar, de forma contínua, a demonstração de conformidade em auditoria, a confiança dos clientes e o cumprimento do RGPD da UE, da Diretiva NIS2 da UE e da DORA da UE.

2. Âmbito

2.1 Esta política aplica-se a todos os sistemas e utilizadores da organização, incluindo:

2.1.1 Postos de trabalho, computadores portáteis, servidores, firewalls, switches, routers e pontos de acesso sem fios

2.1.2 Serviços na nuvem utilizados nas operações empresariais (por exemplo, correio eletrónico, armazenamento de ficheiros, cópias de segurança e ferramentas de colaboração)

2.1.3 Funcionalidades de registo em software antivírus, aplicações, sistemas operativos e equipamentos de rede

2.1.4 Todos os trabalhadores, contratados e prestadores de serviços geridos (MSP) que utilizem ou administrem sistemas

2.1.5 Qualquer local onde sejam utilizados sistemas de TI da empresa, incluindo ambientes remotos, híbridos ou Bring Your Own Device (BYOD)

2.2 A política aplica-se igualmente aos registos gerados por serviços de terceiros relativamente aos quais a organização disponha de acesso administrativo ou de direitos de auditoria contratuais.

3. Objetivos

3.1 Assegurar o registo da atividade dos sistemas, incluindo autenticação, alterações de configuração, acesso a dados sensíveis e alertas de segurança

3.2 Manter registos seguros e exatos para detetar violações da política, erros de sistema ou ações não autorizadas

3.3 Permitir a revisão célere de registos durante incidentes, investigações e auditorias

3.4 Assegurar a sincronização temporal para garantir a integridade e a correlação dos dados de registo

3.5 Proteger os registos contra adulteração, perda ou eliminação prematura

3.6 Cumprir obrigações legais e regulamentares relativas à responsabilização, rastreabilidade e resposta a violações dos sistemas

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Aprova esta política e assegura a sua implementação em todos os sistemas empresariais

4.1.2 Revê alertas de severidade elevada e constatações graves de auditoria comunicadas pelas funções de TI ou de privacidade

4.1.3 Aprova exceções sempre que o registo ou a retenção não possam ser aplicados por limitações técnicas

4.2 Prestador de Suporte de TI / Função interna de TI

4.2.1 Implementa e configura o registo em sistemas operativos, dispositivos de rede, ferramentas antivírus e aplicações críticas

4.2.2 Assegura que os registos são retidos, sujeitos a cópia de segurança e protegidos contra alteração

4.2.3 Revê os registos de forma programada e investiga atividade suspeita ou não autorizada

4.2.4 Mantém sistemas de alerta que sinalizem comportamentos anómalos ou indicadores de intrusão

[... 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 anual

9.1.1 Esta política deve ser revista pelo menos anualmente pelo Diretor-Geral, com o apoio do Prestador de Suporte de TI e do Coordenador de Privacidade.

9.2 Fatores desencadeadores de revisão

9.2.1 Devem ser realizadas revisões extraordinárias em resposta a:

9.2.1.1 Constatações relacionadas com registos provenientes de auditorias internas ou externas

9.2.1.2 Incidentes de segurança em que os registos estivessem em falta, corrompidos ou fossem insuficientes

9.2.1.3 Alterações materiais à infraestrutura de TI (por exemplo, migração para plataformas de registo na nuvem)

9.2.1.4 Atualizações de obrigações legais ou regulamentares (por exemplo, RGPD da UE, Diretiva NIS2 da UE, DORA da UE)

9.3 Controlo de versões

9.3.1 Todas as alterações a esta política devem ser registadas com número da versão, data e resumo das revisões

9.3.2 As versões anteriores devem ser arquivadas e retidas durante, pelo menos, 3 anos

9.3.3 As políticas atualizadas devem ser comunicadas às partes interessadas afetadas, especialmente às que disponham de acesso ao nível do sistema

10. Políticas relacionadas e articulações

10.1 Esta política suporta diretamente e é suportada pelas seguintes políticas SME de segurança da informação:

10.1.1 P17S – Política de proteção de dados e privacidade: Assegura que os dados de registo que contenham informação pessoal são geridos com integridade, retenção e salvaguardas de acesso em conformidade com os requisitos do RGPD da UE.

10.1.2 P21S – Política de Segurança de Rede: Fornece a base para a recolha de registos relacionados com firewalls, acesso sem fios, VPN e monitorização da segmentação.

10.1.3 P24S – Política de desenvolvimento seguro: Assegura que os registos de aplicações (por exemplo, de tentativas de autenticação, erros e exceções) são incorporados na conceção e operação do software.

10.1.4 P30S – Política de Resposta a Incidentes: Depende de dados de registo exatos e completos para detetar, analisar e responder a eventos de segurança da informação.

10.1.5 P23S – Política de sincronização temporal: Assegura marcas temporais consistentes e rastreáveis em todos os sistemas, permitindo correlacionar registos durante investigações.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 8 – Exige a implementação de controlos operacionais para mitigar riscos de segurança da informação, incluindo o registo.

11.2 ISO/IEC 27002

11.2.1 Controlo 8.15 – Exige o registo de eventos para apoiar a deteção de anomalias e a responsabilização.

11.2.2 Controlo 8.16 – Exige a proteção dos registos contra adulteração e acesso não autorizado.

11.2.3 Controlo 8.17 – Exige a monitorização de sistemas quanto a atividade invulgar e a confirmação da eficácia dos controlos de monitorização.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 a AU-12 – Abrangem o conteúdo dos registos de auditoria, revisão, retenção e alertas automatizados.

11.3.2 SI-4 – Exige a deteção de anomalias do sistema e a comunicação de eventos suspeitos.

11.4 RGPD da UE

11.4.1 Artigo 5(1)(f) – Exige a integridade e confidencialidade dos dados pessoais, o que inclui o registo de acessos.

11.4.2 Artigo 32 – Impõe medidas técnicas e organizativas para assegurar a segurança, incluindo registo e monitorização.

11.4.3 Artigo 33 – Exige a notificação atempada de violações, suportada por registos que permitam a análise da causa raiz.

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(d) – Exige mecanismos de registo que detetem anomalias e prestem apoio durante investigações de incidentes.

11.5.2 Artigo 23 – Impõe a comunicação de incidentes no prazo de 24 horas, o que depende de dados de registo exatos e atempados.

11.6 DORA da UE

11.6.1 Artigo 10 – Exige resiliência operacional digital, incluindo a rastreabilidade de incidentes relacionados com TIC através do registo.

11.6.2 Artigo 15 – Obriga à monitorização de prestadores de serviços, incluindo direitos de acesso e revisão de registos.

11.7 COBIT 2019

11.7.1 DSS01.03 – Exige a rastreabilidade da atividade dos sistemas através de registo e monitorização.

11.7.2 DSS05.02 – Trata o registo como um controlo essencial na proteção contra malware e outra atividade não autorizada.