					Insira aqui a designação da entidade jurídica registada							
Número do documento: P20S					Título do documento: **Política de proteção de endpoints contra malware**							
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 para proteção contra malware
ISO/IEC 27002:2022	Controlo 8	Medidas de controlo para proteção de endpoints
NIST SP 800-53 Rev.5	SI-3, SI-4	Proteção contra código malicioso e resposta a incidentes
Diretiva NIS2 da UE	Artigos 21(2)(d), (e)	Malware e gestão de riscos para entidades essenciais e importantes
DORA da UE	Artigos 10(1), 15	Resiliência operacional e verificação de terceiros
COBIT 2019	DSS05.02, DSS05.04	Proteção de endpoints e rede e monitorização
RGPD da UE	Artigos 32(1)(b), 33	Medidas técnicas e organizativas e notificação de violação

1. Finalidade

1.1 Esta política define os requisitos mínimos técnicos, processuais e comportamentais para proteger todos os endpoints — como computadores portáteis, computadores de secretária, dispositivos móveis e suportes amovíveis — contra código malicioso, incluindo vírus, ransomware, spyware, rootkits e outras ameaças de malware.

1.2 A sua finalidade é assegurar que os endpoints são equipados, mantidos e utilizados de forma a reduzir o risco de infeção por malware, a sua propagação e o comprometimento de sistemas.

1.3 A organização reconhece que os endpoints são pontos de entrada comuns para malware e devem, por isso, ser reforçados, monitorizados e protegidos através de múltiplas camadas de defesa.

1.4 Esta política apoia os objetivos de certificação ISO/IEC 27001:2022 da organização e está alinhada com o RGPD da UE, a Diretiva NIS2 da UE, o DORA da UE e outros referenciais aplicáveis.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os endpoints da organização, incluindo computadores de secretária, computadores portáteis, tablets, telemóveis e terminais de ponto de venda

2.1.2 Dispositivos pessoais (BYOD) utilizados para aceder a aplicações empresariais ou dados

2.1.3 Dispositivos de armazenamento amovível, como unidades USB e discos rígidos externos

2.1.4 Quaisquer sistemas operativos, software de endpoint ou ferramentas de comunicação em execução nestas plataformas

2.2 Aplica-se igualmente a:

2.2.1 Colaboradores internos, contratados, estagiários e prestadores de serviços geridos

2.2.2 Dispositivos utilizados no local, remotamente ou em regime de trabalho híbrido

2.2.3 Endpoints ligados à nuvem ou offline que armazenem dados do negócio ou dados pessoais

3. Objetivos

3.1 Prevenir a infeção por malware e a sua propagação através dos sistemas internos, dispositivos dos utilizadores e ligações externas

3.2 Detetar e conter rapidamente ameaças relacionadas com malware através de tecnologias automatizadas de segurança de endpoints e fluxos de escalonamento definidos

3.3 Assegurar que apenas dispositivos autorizados, protegidos e monitorizados são utilizados para aceder à informação do negócio

3.4 Estabelecer responsabilidades claras para os colaboradores e regras de conduta para os utilizadores, de modo a reduzir o risco de incidentes relacionados com malware

3.5 Manter registos rastreáveis e auditáveis de deteções de malware, resposta a incidentes e cumprimento da política

3.6 Proteger dados pessoais e dados do negócio contra comprometimento devido a malware, através de estratégias de defesa em profundidade

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 É responsável por esta política e assegura a disponibilidade de recursos suficientes para a proteção de endpoints

4.1.2 Aprova software antivírus, ferramentas de gestão de dispositivos móveis (MDM) e regras de acesso de terceiros

4.1.3 Revê relatórios de incidentes de malware, resumos de impacto e notificações de violação que envolvam endpoints

4.2 Prestador de suporte de TI / Administrador interno de TI

4.2.1 Seleciona e implementa software antivírus, antimalware e soluções de deteção e resposta em endpoints (EDR)

4.2.2 Assegura que as atualizações são aplicadas de forma consistente e que os registos são conservados

4.2.3 Responde a alertas de malware, isola sistemas infetados e conduz a remediação

4.2.4 Aplica controlos sobre a utilização de USB e de dispositivos externos

[... 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 Requisito de revisão anual

9.1.1 Esta política deve ser formalmente revista pelo menos uma vez por ano pelo Diretor-Geral, em coordenação com o Prestador de suporte de TI e o Coordenador de privacidade

9.2 Atualizações desencadeadas por eventos

9.2.1 A política também deve ser atualizada quando:

9.2.1.1 Uma nova ameaça de malware relevante ou um surto afetar endpoints utilizados pela organização

9.2.1.2 As ferramentas de antivírus ou EDR forem alteradas, atualizadas ou substituídas

9.2.1.3 Um incidente de malware revelar fragilidades no âmbito ou na aplicação desta política

9.2.1.4 Os requisitos legais ou regulamentares (por exemplo, RGPD da UE, DORA da UE, Diretiva NIS2 da UE) forem atualizados

9.3 Controlo de versões e comunicação

9.3.1 Todas as alterações à política devem ser documentadas com número da versão, data e resumo das alterações

9.3.2 O pessoal deve ser notificado das atualizações, especialmente se estas alterarem requisitos operacionais ou comportamentais

9.3.3 As versões anteriores devem ser conservadas no arquivo de políticas durante pelo menos 3 anos para suportar auditorias

10. Políticas relacionadas e interdependências

10.1 Esta política deve ser implementada em conjunto com as seguintes políticas SME:

10.1.1 P9S – Política de trabalho remoto: assegura que os requisitos de proteção de endpoints são aplicados a dispositivos utilizados fora das instalações ou em contextos híbridos

10.1.2 P12S – Política de Gestão de Ativos: suporta o acompanhamento e controlo de todos os endpoints, assegurando que apenas dispositivos autorizados e protegidos são utilizados

10.1.3 P17S – Política de proteção de dados e privacidade: reforça a prevenção de malware como controlo essencial de privacidade para proteger dados pessoais e sensíveis contra comprometimento

10.1.4 P22S – Política de Registo e Monitorização: estabelece os requisitos para o registo de eventos de malware e a manutenção da visibilidade dos alertas para resposta precoce

10.1.5 P30S – Política de Resposta a Incidentes (P30): define as etapas de escalonamento, contenção e notificação externa caso o malware conduza a comprometimento de dados ou interrupção operacional

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Requer a implementação de controlos operacionais para reduzir riscos como ataques de malware

11.2 ISO/IEC 27002

11.2.1 Controlo 8.7 – Detalha práticas de controlo de malware, incluindo antivírus, análise em tempo real, atualizações e formação de utilizadores

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Requer a implementação de mecanismos de proteção contra código malicioso nos endpoints

11.3.2 SI-4 – Exige ações de monitorização, deteção, análise e resposta para ameaças e alertas ao nível do endpoint

11.4 RGPD da UE

11.4.1 Artigo 32(1)(b) – Requer controlos técnicos e organizativos (como antivírus) para proteger dados pessoais

11.4.2 Artigo 33 – Obriga à notificação de violação quando o malware compromete a integridade, confidencialidade ou disponibilidade dos dados

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(d) – Requer medidas para prevenir e responder a ameaças de malware em entidades essenciais e importantes

11.5.2 Artigo 21(2)(e) – Exige estratégias de gestão do risco de cibersegurança em camadas, incluindo proteção de endpoints contra malware

11.6 DORA da UE

11.6.1 Artigo 10(1) – Requer que os sistemas de TIC sejam protegidos contra malware e outras ameaças no âmbito da resiliência operacional

11.6.2 Artigo 15 – Obriga as organizações financeiras a verificar a proteção contra malware junto de prestadores de serviços terceiros

11.7 COBIT 2019

11.7.1 DSS05.02 – Enfatiza medidas de proteção para defender endpoints e redes contra ameaças de malware

11.7.2 DSS05.04 – Suporta a monitorização e emissão de alertas sobre eventos de segurança relacionados com malware no âmbito das operações contínuas