					Insira aqui a designação da entidade jurídica registada							
Número do documento: P20					Título do documento: **Política de Proteção de Endpoints e 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	Exige controlos de proteção de endpoints e proteção contra malware para cumprir os objetivos do SGSI
ISO/IEC 27002:2022	Controlos 8.7, 8	Fornece controlos técnicos e orientações para antimalware, proteção de endpoints e gestão de incidentes
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Define requisitos de proteção contra código malicioso, monitorização centralizada e configuração de referência
RGPD da UE	Artigo 32	Exige medidas técnicas adequadas para proteger dados pessoais, incluindo proteção contra malware
Diretiva NIS2 da UE	Artigo 21(2)(d)	Exige a implementação de medidas de deteção de ameaças ao nível do endpoint e de medidas preventivas
DORA da UE	Artigo 9	Exige gestão do risco das TIC para malware e defesa contra ameaças com origem em endpoints
COBIT 2019	DSS05.01, DSS01.04, MEA	Exige proteção, monitorização e avaliação dos controlos de endpoint

1. Finalidade

1.1 A presente política define os controlos obrigatórios e os requisitos operacionais para proteger os endpoints da organização, incluindo computadores de secretária, computadores portáteis, dispositivos móveis e servidores, contra malware e ameaças relacionadas.

1.2 Estabelece normas mínimas para proteção de endpoints, deteção de malware, resposta de contenção e monitorização comportamental, assegurando que os sistemas permanecem resilientes face a variantes de malware comuns e avançadas.

1.3 A política suporta diretamente o cumprimento da ISO/IEC 27001:2022, Cláusula 8.1, e do Controlo 8.7 do Anexo A, e está alinhada com obrigações regionais de cibersegurança ao abrigo 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 endpoints, incluindo:

2.1.1 Computadores de secretária, computadores portáteis, dispositivos móveis e instâncias virtuais detidos ou geridos pela organização

2.1.2 Dispositivos pessoais autorizados ao abrigo da política Traga o Seu Próprio Dispositivo (BYOD), sujeitos à instalação de MDM ou de agente de endpoint

2.1.3 Servidores e ativos de infraestrutura, incluindo máquinas virtuais alojadas na nuvem e dispositivos periféricos

2.1.4 Sistemas operativos, controladores, serviços locais, agentes de endpoint e controlos de segurança instalados em cada nó

2.2 Estão abrangidos por esta política todos os colaboradores com responsabilidade administrativa, técnica ou operacional sobre qualquer endpoint, incluindo:

2.2.1 Trabalhadores internos e contratados

2.2.2 Prestadores de serviços geridos (MSP), equipas externalizadas de suporte ao posto de trabalho e administradores de TI de terceiros

2.2.3 Utilizadores autorizados a operar sistemas portáteis, computadores portáteis com VPN ativa ou acesso móvel às redes da organização

2.3 A cobertura de ameaças ao abrigo desta política inclui, sem limitar:

2.3.1 Vírus, worms, trojans, ransomware, spyware, rootkits, adware, keyloggers e botnets

2.3.2 Malware sem ficheiros, payloads zero-day, malware para elevação de privilégios e kits de exploração de navegador

2.3.3 Código malicioso entregue através de suportes amovíveis, vetores de phishing, transferências drive-by ou ataques baseados em USB

3. Objetivos

3.1 Proteger a Confidencialidade, Integridade e Disponibilidade dos sistemas endpoint e dos dados por eles tratados através de mecanismos fiáveis de prevenção, deteção e resposta a malware.

3.2 Prevenir a execução ou propagação de código malicioso nas redes da organização mediante a aplicação de salvaguardas técnicas, configurações de endurecimento de referência e telemetria em tempo real.

3.3 Integrar a proteção de endpoints com outros controlos do SGSI, incluindo gestão de vulnerabilidades, controlo de acesso, registo e monitorização, e resposta a incidentes.

3.4 Assegurar visibilidade contínua sobre os endpoints através de plataformas de proteção geridas centralmente, incluindo agentes antivírus/antimalware, Deteção e Resposta em Endpoints (EDR) e telemetria de SIEM.

3.5 Cumprir requisitos legais, regulamentares e normativos que imponham segurança de endpoints (por exemplo, Artigo 32 do RGPD da UE, Artigo 21 da Diretiva NIS2 da UE e Artigo 9 da DORA da UE).

3.6 Definir papéis com responsabilização atribuída, aplicar Acordos de Nível de Serviço (SLA) para aplicação de patches e resposta a alertas, e assegurar a demonstração de conformidade em auditoria através de documentação e reporte.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É responsável por esta política e assegura o seu alinhamento com o SGSI e com a estratégia global de segurança.

4.1.2 Revê trimestralmente as métricas de proteção de endpoints, as tendências de incidentes e a eficácia das ferramentas.

4.1.3 Aprova exceções e aceitações de risco residual relacionadas com a cobertura de endpoints.

4.2 Responsável pela Segurança de Endpoints / Gestor do SOC

4.2.1 Gere os sistemas de proteção de endpoints (por exemplo, AV, EDR, MDM).

4.2.2 Supervisiona a aplicação da política, o ajuste da deteção de ameaças e os playbooks de resposta.

4.2.3 Mantém estatísticas de cobertura, registos de incidentes de malware e configurações de referência de alertas.

[... 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 quando:

9.1.1 Ocorram campanhas de malware de grande escala ou incidentes de segurança de endpoints

9.1.2 Novos tipos de ameaças (por exemplo, malware sem ficheiros, variantes de ransomware) exijam estratégias atualizadas de deteção ou resposta

9.1.3 As plataformas de proteção de endpoints ou as arquiteturas de agentes sofram alterações significativas

9.1.4 Sejam atualizados requisitos legais ou regulamentares que afetem os controlos de endpoint

9.2 A revisão deve ser iniciada pelo Responsável pela Segurança de Endpoints e coordenada com as funções de CISO, Jurídico, Risco e Auditoria.

9.3 As revisões aprovadas devem ser documentadas no registo de controlo documental do SGSI, receber um novo identificador de versão e ser comunicadas a todas as partes afetadas.

9.4 As versões substituídas devem ser arquivadas, ter o acesso restringido e ser conservadas para assegurar a integridade do rasto de auditoria de acordo com os prazos de retenção do SGSI.

10. Políticas relacionadas e ligações

10.1 P1 - Política de Segurança da Informação. Estabelece os princípios fundamentais para a proteção de sistemas, dados e redes. A presente política aplica esses princípios ao nível do endpoint através de controlos técnicos e processuais de proteção contra malware.

10.2 P4 - Política de Controlo de Acesso. Define restrições de acesso de utilizadores aplicadas na camada de endpoint, incluindo proteções contra elevação de privilégios e instalações não autorizadas de software não validado.

10.3 P5 - Política de Gestão de Alterações. Assegura que as atualizações ao software de proteção de endpoints, às regras de política ou às configurações de agentes ficam sujeitas a processos de aprovação e implementação controlada.

10.4 P12 - Política de Gestão de Ativos. Fornece a linha de base de classificação de ativos e inventário necessária para a visibilidade de endpoints, cobertura de patches e definição do âmbito da proteção contra malware.

10.5 P22 - Política de Registo e Monitorização. Permite a integração de alertas de endpoint, estado operacional dos agentes e inteligência sobre ameaças em sistemas de SIEM centralizados para deteção em tempo real e rastreabilidade forense.

10.6 P30 - Política de Resposta a Incidentes (P30). Liga os incidentes de malware com origem em endpoints a fluxos de trabalho normalizados de contenção, erradicação, investigação e recuperação, com papéis atribuídos e limiares de escalonamento.

11. Normas e quadros de referência

11.1 ISO/IEC 27001:

11.1.1 Cláusula 8.1 - Planeamento e controlo operacionais: exige a implementação de controlos técnicos, incluindo salvaguardas de endpoint, para manter os objetivos do SGSI.

11.2 ISO/IEC 27002:2022 - Controlos 8.7, 8:

11.2.1 Fornece orientações técnicas detalhadas sobre medidas antimalware, implementação segura de software, monitorização e preparação para incidentes em ambientes de endpoint.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Proteção contra código malicioso: exige a utilização de ferramentas antimalware com análise em tempo real, no acesso e comportamental.

11.3.2 SI-4 - Monitorização de sistemas: suporta a integração de telemetria com plataformas centralizadas de deteção.

11.3.3 CM-6 - Definições de configuração: reforça definições de configuração de referência em endpoints, incluindo a aplicação de agentes de proteção.

11.4 RGPD da UE (2016/679):

11.4.1 Artigo 32 - Segurança do Tratamento: exige que as organizações implementem medidas técnicas adequadas para proteger dados pessoais, incluindo proteção contra ameaças de malware.

11.5 Diretiva NIS2 da UE (2022/2555):

11.5.1 Artigo 21(2)(d): obriga as entidades a implementar medidas de deteção e prevenção de ameaças, incluindo mecanismos de defesa contra malware ao nível do endpoint.

11.6 DORA da UE (2022/2554):

11.6.1 Artigo 9 - Requisitos de gestão do risco das TIC: exige que as entidades financeiras adotem medidas de proteção para prevenir, detetar e responder a malware e a ameaças com origem em endpoints.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Protect Against Malware: exige a deteção e mitigação de malware em todos os endpoints da organização.

11.7.2 DSS01.04 - Manage Availability and Capacity: assegura que a proteção contra malware é equilibrada com o desempenho do sistema e a continuidade do negócio.

11.7.3 MEA03 - Monitor, Evaluate and Assess Compliance: exige auditorias periódicas aos controlos de endpoint e à eficácia da proteção.