					Insira aqui a designação da entidade jurídica registada							
Número do documento: P19					Título do documento: **Política de Gestão de Vulnerabilidades e de Patches**							
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	Tratamento sistemático de vulnerabilidades técnicas; eficácia contínua dos controlos de segurança.
ISO/IEC 27002:2022	Controlos 8.8, 8.9, 5	Orientações de implementação para aplicação de patches, varrimentos de vulnerabilidades, integridade do software, configuração segura e inventário de ativos.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Varrimentos frequentes, remediação de falhas e gestão da configuração aplicados.
RGPD da UE	Artigo 32, Considerando 49	Medidas técnicas para aplicação atempada de patches, tratamento de vulnerabilidades e continuidade da segurança.
Diretiva NIS2 da UE	Artigo 21(2)(d)	Deteção, resposta e mitigação de vulnerabilidades para um elevado nível de higiene de cibersegurança.
DORA da UE	Artigos 8, 10(2)(f)	Remediação atempada de vulnerabilidades das TIC; avaliações contínuas orientadas por ameaças.
COBIT 2019	DSS05.02, DSS01.03, MEA	Varrimento/acompanhamento/mitigação de fraquezas técnicas; monitorização de exploração; auditoria da eficácia, incluindo o estado dos patches.

1. Finalidade

1.1 A presente política define os requisitos obrigatórios da organização para identificar, classificar, remediar e monitorizar vulnerabilidades técnicas e falhas de software em todos os sistemas de informação e ativos abrangidos pelo Sistema de Gestão da Segurança da Informação (SGSI).

1.2 Assegura que todas as vulnerabilidades conhecidas são avaliadas e tratadas de forma atempada e com base no risco, através da aplicação coordenada de patches, ajustamentos de configuração ou controlos compensatórios, em alinhamento com as necessidades do negócio e as obrigações de conformidade.

1.3 Esta política suporta o cumprimento do controlo 8.8 do Anexo A da ISO/IEC 27001 e das orientações da ISO/IEC 27002, e responde aos requisitos regulamentares do artigo 8 do DORA da UE, do artigo 21 da Diretiva NIS2 da UE, do artigo 32 do RGPD da UE e dos domínios DSS e APO do COBIT 2019.

2. Âmbito

2.1 Esta política aplica-se a todos os sistemas de informação, ativos e ambientes que armazenem, tratem ou transmitam dados sujeitos à governação do SGSI, incluindo:

2.1.1 Sistemas operativos, aplicações, dispositivos de rede, firmware, plataformas de computação em nuvem, APIs e software de terceiros.

2.1.2 Sistemas em ambientes de desenvolvimento, pré-produção, produção, cópia de segurança e recuperação de desastre.

2.1.3 Endpoints, servidores, dispositivos de Internet das Coisas (IoT), infraestrutura de virtualização e contentores.

2.2 É vinculativa para:

2.2.1 Pessoal interno: administradores de TI, engenheiros de sistemas, programadores de aplicações, analistas de segurança e equipas de infraestrutura.

2.2.2 Partes externas: contratados, prestadores de serviços geridos (MSP), fornecedores de software e integradores de sistemas com responsabilidades técnicas sobre os ativos abrangidos.

2.3 A política abrange o ciclo de vida completo de vulnerabilidades e patches, incluindo:

2.3.1 Varrimento e deteção

2.3.2 Classificação e priorização do risco

2.3.3 Aquisição, teste, implementação e reversão de patches

2.3.4 Tratamento de exceções e planeamento de controlos compensatórios

2.3.5 Registo, reporte e rastreabilidade para auditoria

3. Objetivos

3.1 Assegurar que todas as vulnerabilidades conhecidas são identificadas, avaliadas e remediadas de forma a minimizar a exposição ao risco e a alinhar-se com as prioridades operacionais.

3.2 Estabelecer processos consistentes e transversais à organização para varrimentos de vulnerabilidades, classificação da severidade (por exemplo, CVSS) e gestão de patches, incluindo tratamento de emergência e planeamento de reversão.

3.3 Permitir uma gestão segura da configuração através do alinhamento com configurações de referência de hardening, práticas de controlo de alterações e inteligência sobre ameaças em tempo real.

3.4 Proporcionar conformidade mensurável com os controlos regulamentares e normativos relacionados com a integridade dos sistemas, a higiene de patches e a remediação atempada de falhas.

3.5 Definir autoridade e responsabilização entre funções ao longo de todo o ciclo de vida da gestão de vulnerabilidades, assegurando que todas as partes interessadas atuam dentro dos SLA definidos e das métricas de controlo reportáveis.

3.6 Reforçar a capacidade de demonstrar conformidade em auditoria e melhorar a resiliência face a ameaças emergentes, incluindo vulnerabilidades zero-day, cadeias ativas de exploração e divulgações críticas de fornecedores.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É responsável pela política e assegura a sua integração no SGSI.

4.1.2 Define a postura de risco da organização e assegura o alinhamento com as expectativas regulamentares e de controlo.

4.2 Responsável pela Gestão de Vulnerabilidades / Gestor de Operações de Segurança

4.2.1 Supervisiona as operações de gestão de vulnerabilidades e de patches, de ponta a ponta.

4.2.2 Coordena os calendários de varrimento, os modelos de priorização e os prazos de remediação.

4.2.3 Mantém o Registo de Vulnerabilidades e colabora na avaliação de controlos compensatórios.

[... 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 pelo menos anualmente ou sempre que ocorra:

9.1.1 Atualizações regulamentares significativas (por exemplo, alterações ao DORA da UE, à Diretiva NIS2 da UE)

9.1.2 Alterações aos referenciais de priorização de vulnerabilidades (por exemplo, atualizações do CVSS)

9.1.3 Alterações relevantes no ambiente de TI (por exemplo, migração para a nuvem, reformulação do EDR)

9.1.4 Violações de grande impacto ou alertas externos que exijam o reforço da política

9.2 As revisões devem ser conduzidas pelo CISO em colaboração com Operações de Segurança, Gestão de Riscos e liderança de Infraestrutura.

9.3 As atualizações da política devem ser:

9.3.1 Documentadas no Registo de Controlo Documental do SGSI

9.3.2 Revistas e aprovadas pela gestão de topo

9.3.3 Comunicadas a todas as partes interessadas afetadas, incluindo subcontratantes responsáveis pelo tratamento

9.4 As versões históricas devem ser conservadas de forma segura para efeitos de auditoria e responsabilização.

10. Políticas relacionadas e interligações

10.1 P1 - Política de Segurança da Informação. Estabelece o compromisso global de proteger sistemas e dados, incluindo a gestão proativa de vulnerabilidades e a garantia da integridade do software.

10.2 P5 - Política de Gestão de Alterações. Rege toda a implementação de patches e ajustamentos de configuração, exigindo documentação, testes, aprovação e procedimentos de reversão que complementam os processos de remediação de vulnerabilidades.

10.3 P6 - Política de Gestão de Riscos. Suporta a classificação e o tratamento de vulnerabilidades não remediadas através de avaliações de risco estruturadas, análise de impacto e procedimentos de aceitação do risco residual.

10.4 P12 - Política de Gestão de Ativos. Assegura que os sistemas são inventariados e classificados com rigor, permitindo varrimentos de vulnerabilidades consistentes, atribuição de titularidade e cobertura de patches ao longo do ciclo de vida.

10.5 P22 - Política de Registo e Monitorização. Define requisitos para a deteção de eventos e a geração de rasto de auditoria. Esta política suporta a visibilidade sobre atividades de aplicação de patches, alterações não autorizadas e tentativas de exploração dirigidas a vulnerabilidades conhecidas.

10.6 P30 - Política de Resposta a Incidentes (P30). Especifica protocolos de escalonamento e estratégias de contenção para vulnerabilidades exploradas, investigações de violações e ações corretivas alinhadas com os controlos desta política.

11. Normas e quadros de referência

11.1 ISO/IEC 27001: Cláusula 8.1 - Planeamento e controlo operacional: exige o tratamento sistemático de vulnerabilidades técnicas para assegurar a eficácia contínua dos controlos de segurança.

11.2 ISO/IEC 27002:2022 - Controlos 8.8, 8.9, 5: fornece orientações de implementação para aplicação de patches, varrimento de vulnerabilidades, integridade do software e integração com configuração segura e inventário de ativos.

11.3 NIST SP 800-53 Rev.5: RA-5 - Monitorização e varrimento de vulnerabilidades: determina a realização frequente de varrimentos e o acompanhamento da remediação. SI-2 - Remediação de falhas: exige a avaliação e mitigação atempadas de falhas com patches disponíveis ou outras ações. CM-2 / CM-6 - Linhas de base e controlos de gestão da configuração: estabelece a base para configurações seguras dos sistemas ligadas à aplicação de patches.

11.4 RGPD da UE (2016/679): Artigo 32 - Segurança do Tratamento: exige a implementação de medidas técnicas adequadas, como a aplicação atempada de patches e o tratamento de vulnerabilidades, para assegurar a confidencialidade e a resiliência dos sistemas. Considerando 49: incentiva as entidades a implementar controlos preventivos contra ameaças conhecidas para suportar a segurança e a continuidade.

11.5 Diretiva NIS2 da UE (2022/2555): Artigo 21(2)(d): obriga as entidades essenciais e importantes a detetar, responder e mitigar vulnerabilidades dos sistemas e a manter um elevado nível de higiene de cibersegurança.

11.6 DORA da UE (2022/2554): Artigo 8 - Gestão do risco das TIC: exige a identificação e remediação atempada de vulnerabilidades nas tecnologias da informação e comunicação utilizadas em sistemas financeiros. Artigo 10(2)(f): salienta avaliações contínuas de vulnerabilidades orientadas por ameaças e a aplicação de patches como parte da resiliência operacional.

11.7 COBIT 2019: DSS05.02 - Gerir Vulnerabilidades de Segurança: orienta as organizações a varrer, acompanhar e mitigar fraquezas técnicas conhecidas. DSS01.03 - Monitorizar Infraestrutura: assegura que os sistemas são monitorizados quanto a sinais de exploração ou fraqueza. MEA03 - Monitorização, Avaliação e Análise da Conformidade: exige auditoria regular da eficácia dos controlos, incluindo o estado dos patches e o tratamento de exceções.