					Insira aqui a designação da entidade jurídica registada							
Número do documento: P19S					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	
ISO/IEC 27002:2022	Controlos 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
Diretiva NIS2 da UE	Artigos 21(2)(d), 21(2)(e)	
DORA da UE	Artigos 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
RGPD da UE	Artigo 32(1)(b)	

1. Finalidade

1.1 A presente política define a forma como a organização identifica, avalia e mitiga vulnerabilidades em sistemas, aplicações e infraestrutura.

1.2 A sua finalidade é reduzir o risco de cibersegurança através da imposição de práticas atempadas de aplicação de patches e de remediação com base no risco, adequadas a pequenas e médias empresas (PME).

1.3 Esta política apoia o cumprimento dos requisitos de certificação ISO/IEC 27001:2022 e contribui para o cumprimento das obrigações regulamentares ao abrigo do RGPD da UE, da Diretiva NIS2 da UE e do DORA da UE, exigindo a gestão proativa de vulnerabilidades técnicas.

1.4 A organização reconhece que sistemas sem patches aplicados constituem uma ameaça significativa à segurança da informação e devem ser tratados de forma sistemática e sem demora.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os servidores, computadores de secretária, computadores portáteis, dispositivos móveis, equipamentos de rede e plataformas alojadas na nuvem utilizados pela organização

2.1.2 Todos os sistemas operativos, software de terceiros, extensões e aplicações utilizados nas operações da organização

2.1.3 Todo o pessoal interno de TI ou prestadores externos de serviços de TI responsáveis pela manutenção, atualização ou monitorização de sistemas

2.1.4 Qualquer código desenvolvido à medida ou software incorporado mantido pela organização ou em seu nome

2.2 A política abrange tanto a infraestrutura gerida diretamente pela organização como os sistemas administrados por fornecedores contratados ou prestadores de serviços de alojamento.

3. Objetivos

3.1 Identificar e avaliar vulnerabilidades conhecidas em todos os ativos de TI de forma atempada e consistente

3.2 Aplicar patches e atualizações de software com base na severidade e no risco para as operações da organização ou para os dados pessoais

3.3 Prevenir a exploração de fraquezas técnicas que possam conduzir à interrupção de serviços, violação de dados ou incumprimento legal

3.4 Manter registos exatos dos patches aplicados, questões pendentes e exceções para assegurar a demonstração de conformidade em auditoria

3.5 Utilizar ferramentas e processos adequados à dimensão e complexidade operacional da organização, sem comprometer a eficácia

3.6 Apoiar o cumprimento legal e regulamentar, incluindo o Artigo 32 do RGPD da UE e o Controlo 8 do Anexo A da ISO/IEC 27001

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Detém a responsabilidade global por assegurar que as atividades de gestão de vulnerabilidades e de aplicação de patches são implementadas

4.1.2 Aprova exceções de risco quando os patches não possam ser aplicados e revê as estratégias de mitigação associadas

4.1.3 Revê os relatórios de estado da aplicação de patches e assegura a disponibilização dos recursos necessários para cumprir as obrigações de atualização

4.2 Prestador de suporte de TI / administrador interno de TI

4.2.1 Monitoriza os sistemas quanto a vulnerabilidades e patches disponíveis através de alertas dos fornecedores, avisos de ameaças e notificações ao nível do sistema operativo

4.2.2 Aplica atualizações de sistema operativo, firmware e aplicações dentro dos prazos definidos

4.2.3 Mantém um registo formal de patches e documenta atualizações não resolvidas ou adiadas

4.2.4 Realiza testes e calendariza atualizações críticas para minimizar a disrupção operacional

[... 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 uma vez por ano pelo Diretor-Geral, com contributos do prestador de TI e do Coordenador de privacidade

9.2 Fatores desencadeadores de revisão

9.2.1 Devem ocorrer revisões intercalares se:

9.2.1.1 Uma vulnerabilidade grave ou exploração afetar sistemas no âmbito desta política

9.2.1.2 Ocorrerem alterações significativas em sistemas ou software

9.2.1.3 Uma auditoria identificar lacunas nos processos de aplicação de patches

9.2.1.4 For registado um incidente ou violação relacionado com a aplicação de patches

9.3 Controlo de versões da política

9.3.1 Todas as atualizações devem ser registadas num registo de versões com um resumo das alterações

9.3.2 As alterações devem ser comunicadas ao pessoal afetado

9.3.3 As versões desatualizadas devem ser arquivadas com acesso restrito

10. Políticas relacionadas e articulações

10.1 Esta política apoia e depende de várias outras políticas SME:

10.1.1 P12S – Política de Gestão de Ativos: Identifica a propriedade e classificação dos sistemas, assegurando que todos os ativos que requerem aplicação de patches são considerados e inventariados

10.1.2 P14S – Política de Retenção e Eliminação de Dados: Assegura que os sistemas planeados para desativação são atualizados de forma segura ou sujeitos a eliminação segura, reduzindo a exposição a vulnerabilidades

10.1.3 P17S – Política de Proteção de Dados e Privacidade: Prioriza a remediação de vulnerabilidades em sistemas que tratam dados pessoais para cumprir a legislação de privacidade

10.1.4 P22S – Política de Registo e Monitorização: Apoia a deteção de sistemas sem patches aplicados ou de comportamentos suspeitos que possam indicar a exploração de uma vulnerabilidade

10.1.5 P30S – Política de Resposta a Incidentes: Define procedimentos para responder a vulnerabilidades que resultem em incidentes de segurança, incluindo etapas de escalonamento e reporte

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Exige a implementação de controlos para tratar o risco operacional, incluindo a gestão de vulnerabilidades

11.2 ISO/IEC 27002

11.2.1 Controlo 8.8 – Especifica processos para identificar e corrigir fraquezas conhecidas nos sistemas

11.2.2 Controlo 8.9 – Dá ênfase à configuração segura, à validação de patches e ao controlo de alterações para evitar novas exposições durante as atualizações

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Exige a identificação de vulnerabilidades e a sua remediação dentro de prazos definidos

11.3.2 SI-2 – Exige a aplicação célere de patches e atualizações com base na severidade

11.3.3 CM-2 – Regula as configurações de referência dos sistemas e a documentação de atualizações para assegurar proteções consistentes

11.4 RGPD da UE

11.4.1 Artigo 32(1)(b) – Exige que as organizações implementem medidas técnicas adequadas, incluindo a aplicação de patches, para manter a segurança do tratamento

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(d) – Exige o tratamento de vulnerabilidades através de varrimento sistemático e remediação

11.5.2 Artigo 21(2)(e) – Impõe a configuração segura e a gestão de patches para assegurar a resiliência das TIC

11.6 DORA da UE

11.6.1 Artigo 8(1) – Exige a deteção e mitigação de riscos das TIC, incluindo vulnerabilidades técnicas

11.6.2 Artigo 10(2) – Impõe às entidades financeiras a remediação de fraquezas que afetem sistemas e operações de TIC

11.7 COBIT 2019

11.7.1 DSS05.02 – Exige o tratamento de vulnerabilidades técnicas conhecidas para manter operações seguras

11.7.2 APO12.01 – Alinha a gestão de riscos com a monitorização proativa e a correção de fraquezas dos sistemas