					Insira aqui a designação da entidade jurídica registada							
Número do documento: P39					Título do documento: **Política de Divulgação Coordenada de Vulnerabilidades**							
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**

Alinhada com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
RGPD da UE	Art. 32(1)(d)	
Diretiva NIS2 da UE	Art. 21(2)(e)	
DORA da UE	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Finalidade

1.1 Estabelecer um processo formal para receber, tratar e divulgar informações sobre vulnerabilidades que afetem os sistemas ou serviços da organização, conforme exigido pelo artigo 21(2)(e) da Diretiva NIS2 da UE, relativo ao tratamento e à divulgação de vulnerabilidades.

1.2 Incentivar investigadores de segurança externos, parceiros e utilizadores a reportarem vulnerabilidades de forma responsável, no âmbito da Divulgação Coordenada de Vulnerabilidades (CVD), e definir a forma como a organização comunica informação sobre vulnerabilidades às partes interessadas.

2. Âmbito

2.1 Esta política aplica-se a todos os sistemas de rede e de informação detidos ou operados pela organização, bem como a quaisquer vulnerabilidades identificadas nesses sistemas.

2.2 Abrange as equipas internas (segurança, TI e desenvolvimento) e quaisquer partes externas que reportem vulnerabilidades (por exemplo, investigadores, clientes e fornecedores). Regula igualmente as comunicações com fornecedores de produtos ou prestadores de serviços quando os seus componentes estejam envolvidos na vulnerabilidade.

3. Objetivos

3.1 Detetar e resolver vulnerabilidades de segurança em tempo útil, recorrendo tanto a avaliações internas como a divulgações externas.

3.2 Fornecer orientações claras para que os autores de reportes externos submetam informação sobre vulnerabilidades de forma segura e lícita, e para que a organização responda e execute a remediação de forma eficaz.

3.3 Assegurar o alinhamento com os requisitos da Diretiva NIS2 da UE e com as melhores práticas do setor (ISO/IEC 29147 e ISO/IEC 30111) para a divulgação coordenada de vulnerabilidades, reforçando a segurança global do ecossistema.

4. Papéis e responsabilidades

4.1 Equipa de Resposta a Vulnerabilidades (VRT): equipa designada (liderada pelo Diretor de Segurança da Informação ou pelo Responsável pela Gestão de Vulnerabilidades) que recebe e tria reportes de vulnerabilidades, avalia o risco e o impacto e coordena a remediação e a divulgação pública.

4.2 Equipas de TI e Desenvolvimento: trabalham com a VRT para validar as vulnerabilidades reportadas, desenvolver e testar patches ou medidas de mitigação, e implementar correções. Fornecem, quando necessário, detalhes técnicos para avisos de segurança.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Monitorização e auditoria

9.1 A VRT deve manter um registo de divulgação de vulnerabilidades, acompanhando cada reporte desde a receção até ao encerramento. Este registo deve ser revisto mensalmente para assegurar o progresso atempado dos itens em aberto. Os itens em atraso devem ser escalados.

9.2 A Auditoria Interna / Função de Conformidade, ou um avaliador de segurança independente, deve analisar anualmente a eficácia do processo de tratamento de vulnerabilidades, por exemplo verificando se amostras de casos de vulnerabilidade foram tratadas de acordo com a política (confirmadas, corrigidas e divulgadas em tempo útil). Deve igualmente ser verificado se o canal público de divulgação está operacional (por exemplo, se mensagens de teste são recebidas e tratadas).

9.3 As métricas sobre vulnerabilidades (volume por severidade, tempos de remediação, etc.) devem ser compiladas trimestralmente e apresentadas ao comité de governação de cibersegurança, para suportar atualizações da avaliação de riscos.

10. Revisão e manutenção

10.1 Esta política deve ser revista, pelo menos, anualmente. Adicionalmente, qualquer alteração significativa no nosso ambiente de TI (por exemplo, lançamento de um novo serviço exposto à Internet) ou evolução regulatória relevante (por exemplo, nova legislação da UE sobre divulgação de vulnerabilidades de produtos) desencadeia uma revisão extraordinária.

10.2 As atualizações à política devem incorporar o feedback dos autores de reportes externos e as lições aprendidas de análises internas pós-incidente. As alterações de maior impacto devem ser aprovadas pelo Diretor de Segurança da Informação e comunicadas a todos os trabalhadores, sendo também publicadas no nosso repositório online de políticas de segurança, por transparência.

11. Políticas relacionadas e ligações

11.1 P01 – Política de Segurança da Informação. Define o mandato de gestão para o tratamento e a divulgação de vulnerabilidades.

11.2 P19 – Política de Gestão de Vulnerabilidades e Patches. Define o fluxo interno de remediação associado à receção de CVD.

11.3 P24 – Política de Desenvolvimento Seguro. Sustenta as correções e o reforço do SDLC com base nos problemas reportados.

11.4 P25 – Política de Requisitos de Segurança das Aplicações. Assegura que os produtos dispõem de requisitos de segurança adequados a processos de divulgação.

11.5 P30 – Política de Resposta a Incidentes. Trata a exploração ativa de vulnerabilidades divulgadas.

11.6 P31 – Política de Recolha de Evidência e Análise Forense. Preserva artefactos associados a falhas reportadas ou exploradas.

11.7 P26 – Política de Segurança de Terceiros e Fornecedores. Coordena divulgações que envolvam componentes de fornecedores.

11.8 P37 – Política de Conformidade Jurídica e Regulamentar. Regula notificações, redação de salvaguardas de proteção e publicação.

12. Referências

12.1 Diretiva NIS2 (UE 2022/2555), artigo 21(2), alínea (e) (segurança no desenvolvimento e tratamento e divulgação de vulnerabilidades)

12.2 Regulamento de Execução (UE) 2024/2690 da Comissão, anexo, secção 6.10 (requisitos técnicos sobre processos de tratamento e divulgação de vulnerabilidades)

12.3 Orientações Técnicas da ENISA sobre Medidas de Gestão do Risco de Cibersegurança – secção relativa a tratamento e divulgação de vulnerabilidades

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (controlo A.5.7 sobre informações sobre ameaças e divulgação de vulnerabilidades; controlo A.8.28 sobre desenvolvimento seguro)

12.5 ISO/IEC 29147:2018 (orientações para divulgação de vulnerabilidades) e ISO/IEC 30111:2019 (orientações para processos de tratamento de vulnerabilidades)