

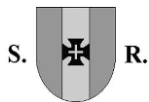


REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Política de Gestão de Vulnerabilidades Técnicas da Direção Regional de Informática (DRI)

Ref. Documento:	POLT-008-DRI- Política_de_Gestao_de_Vulnerabilidades_ Técnicas_v1.1-2026-04-24
Versão:	1.1
Data:	abril de 26
Autor:	DRI
Proprietário	Direção Regional de Informática (DRI)
Classificação:	Pública





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Política de Gestão de Vulnerabilidades Técnicas da Direção Regional de Informática (DRI)

Revisões - Histórico

Versão	Data	Autor da Revisão	Sumário das Alterações
0.1	2026-04-02	DRI-DSTC	Preparação do documento final para aprovação
1.0	2026-04-13	DRI-DSTC	Versão final aprovada
1.1	2026-04-24	DRI-DSTC	Alterações na classificação do documento

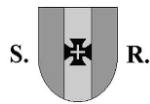
Tabela 1 – Revisões - Histórico

Aprovação

Nome	Cargo	Assinatura	Data
Dr. César Rosa	Diretor Regional de Informática		

Tabela 2 - Aprovação





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Política de Gestão de Vulnerabilidades Técnicas da Direção Regional de Informática (DRI)

Índice

1. INTRODUÇÃO	4
2. OBJETIVOS	4
3. ÂMBITO DE APLICAÇÃO E DESTINATÁRIOS	4
4. POLÍTICA DE GESTÃO DE VULNERABILIDADES TÉCNICAS	5
5. RESPONSABILIDADES	5
6. PROTEÇÃO DE DADOS PESSOAIS	5
7. REVISÃO PERIÓDICA E MELHORIA CONTÍNUA	5
8. DISPOSIÇÕES TRANSITÓRIAS E FINAIS	5
9. GLOSSÁRIO	7
TABELA 1 – REVISÕES - HISTÓRICO	2
TABELA 2 - APROVAÇÃO	2





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Política de Gestão de Vulnerabilidades Técnicas da Direção Regional de Informática (DRI)

1. Introdução

A gestão de vulnerabilidades é um dos pilares fundamentais para a segurança da informação na Direção Regional de Informática (DRI), sendo indispensável para garantir a continuidade dos serviços e a proteção dos ativos digitais. Esta política estabelece as diretrizes para identificar, avaliar, tratar e monitorizar vulnerabilidades nos sistemas e infraestruturas sob responsabilidade da DRI, promovendo um ambiente seguro e resiliente face a ameaças tecnológicas. Ao definir procedimentos claros para a gestão de vulnerabilidades, a DRI reforça o compromisso com as boas práticas de segurança, alinhando-se com normas internacionais e requisitos legais aplicáveis.

2. Objetivos

O objetivo desta política é garantir que todas as vulnerabilidades identificadas nos sistemas, aplicações e dispositivos sob gestão da DRI sejam tratadas de forma eficiente, minimizando riscos para a integridade, disponibilidade e confidencialidade da informação. Para tal, são definidos procedimentos para a deteção, avaliação, priorização e mitigação de vulnerabilidades, assegurando que os serviços críticos permanecem protegidos e que as ações corretivas são implementadas em tempo útil. Esta política visa ainda promover a melhoria contínua dos processos de segurança, contribuindo para a redução do risco tecnológico e para a conformidade com os requisitos normativos e legais.

A implementação desta política permite reduzir impactos financeiros, reputacionais e operacionais decorrentes de vulnerabilidades exploradas por agentes maliciosos. Ao estabelecer mecanismos robustos de gestão de vulnerabilidades, a DRI procura assegurar que as operações críticas permanecem seguras, mesmo perante ameaças emergentes, como ataques de *ransomware*, exploração de falhas ou incidentes de segurança. Este compromisso é essencial para manter a confiança dos cidadãos e das entidades que dependem dos sistemas geridos pela Direção Regional.

Por fim, esta política incentiva uma cultura organizacional orientada para a prevenção e a resposta eficaz a vulnerabilidades, promovendo práticas consistentes entre equipas técnicas, gestores e utilizadores. A clareza nos procedimentos e responsabilidades assegura que todos os intervenientes compreendem o seu papel na gestão de vulnerabilidades, criando um ambiente mais resiliente e preparado para responder a incidentes de segurança com eficácia e rapidez.

3. Âmbito de aplicação e destinatários

Esta política aplica-se a todos os sistemas, aplicações, bases de dados, dispositivos e infraestruturas sob gestão da DRI, incluindo servidores, postos de trabalho, dispositivos móveis corporativos e serviços em nuvem. Abrange também os fornecedores e parceiros que prestem serviços à DRI, exigindo que atuem em conformidade com as normas internas e cláusulas contratuais relativas à gestão de vulnerabilidades. A política é obrigatória para todos os colaboradores, técnicos e entidades terceiras que tenham acesso ou responsabilidade sobre os ativos digitais da DRI ou geridos por esta.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Política de Gestão de Vulnerabilidades Técnicas da Direção Regional de Informática (DRI)

4. Política de Gestão de Vulnerabilidades Técnicas

A política define que todos os ativos críticos sob gestão da DRI devem ser sujeitos a avaliações periódicas de vulnerabilidades, utilizando ferramentas automatizadas, auditorias e testes de penetração. As vulnerabilidades identificadas devem ser classificadas segundo critérios de risco, priorizadas e tratadas conforme a gravidade e impacto potencial, com atualização e correção de sistemas, aplicações e configurações. A gestão de vulnerabilidades inclui o registo, acompanhamento, comunicação e validação das medidas corretivas, assegurando que os riscos são mitigados de forma eficiente e transparente.

A estratégia de gestão de vulnerabilidades combina diferentes abordagens, como a monitorização contínua, análise de relatórios de fabricantes, participação em programas de divulgação responsável e formação dos colaboradores. A frequência das avaliações e a resposta às vulnerabilidades devem respeitar requisitos legais e operacionais, com atualização imediata para vulnerabilidades críticas e procedimentos definidos para as de menor impacto. O histórico de vulnerabilidades e ações tomadas deve ser documentado e revisto periodicamente para garantir a melhoria contínua dos processos de segurança.

5. Responsabilidades

A implementação desta política de gestão de vulnerabilidades implica uma definição clara das responsabilidades de todos os intervenientes:

- Diretor Regional de Informática: aprova a política de gestão de vulnerabilidades, assegura recursos adequados e supervisiona a implementação dos procedimentos definidos.
- Responsável de Segurança: coordena as atividades de identificação, avaliação, priorização e mitigação de vulnerabilidades, monitoriza a execução das ações corretivas e garante a comunicação eficaz das medidas implementadas.
- Equipas técnicas: realizam avaliações periódicas de vulnerabilidades, aplicam correções e atualizações, registam e reportam incidentes identificados, e colaboram na implementação das ações de mitigação definidas.
- Utilizadores: devem reportar suspeitas de vulnerabilidades, garantir que a informação institucional é armazenada apenas em locais autorizados e seguir as orientações de segurança definidas pela DRI.

6. Proteção de Dados Pessoais

A recolha e tratamento de dados pessoais deve seguir a legislação aplicável, nomeadamente o Regulamento Geral sobre a Proteção de Dados (RGPD), e as diretrizes impostas pelo Gabinete Regional para a Conformidade Digital, Proteção de Dados e Cibersegurança (GCPD).

7. Revisão Periódica e Melhoria Contínua

A política será revista anualmente ou sempre que houver alterações significativas nos sistemas, legislação ou níveis de risco.

8. Disposições Transitórias e Finais

A presente política estará disponível no sítio da DRI em <https://www.madeira.gov.pt/dri>, sendo disso dado conhecimento a todos os destinatários da mesma, sempre que haja alteração significativa, ou aquando da primeira interação com a entidade.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Política de Gestão de Vulnerabilidades Técnicas da Direção Regional de Informática (DRI)

Para clarificar qualquer questão relacionada com a interpretação ou aplicação desta política, pode consultar o responsável de segurança da DRI, através do email: responsavelciberseguranca.dri@madeira.gov.pt.

As entidades terceiras (fornecedores, consultores ou prestadores de serviços) só são consideradas confiáveis quando atuem em conformidade com as políticas internas da DRI, nos termos dos contratos, protocolos e/ou acordos de confidencialidade celebrados.

A violação das disposições constantes desta política, por parte de trabalhadores da DRI, pode dar origem à instauração de processo disciplinar, nos termos da Lei Geral do Trabalho em Funções Públicas, podendo, consoante a gravidade, conduzir à aplicação de sanções disciplinares, incluindo a cessação do vínculo laboral, sem prejuízo de eventual responsabilidade civil ou criminal.

Os fornecedores, consultores ou outros terceiros que violem esta política podem estar sujeitos a sanções contratuais, como a remoção de acessos, rescisão unilateral do contrato por justa causa, ou ainda à responsabilização civil e/ou criminal, nos termos da legislação aplicável.

As disposições constantes do presente documento produzem efeitos a partir da data da sua aprovação formal pelo dirigente máximo do serviço.





9. Glossário

Este glossário define os principais termos relacionados com recursos tecnológicos, referidos na gestão de vulnerabilidades técnicas:

- **Vulnerabilidade:** Falha ou fraqueza em sistemas, processos ou aplicações que pode ser explorada para comprometer a segurança da informação.
- **Gestão de Vulnerabilidades:** Conjunto de processos para identificar, avaliar, priorizar, tratar e monitorizar vulnerabilidades nos ativos tecnológicos da organização.
- **Threat (Ameaça):** Evento ou agente capaz de explorar vulnerabilidades, causando impactos negativos na organização.
- **Exploit:** Código ou técnica utilizada para tirar partido de uma vulnerabilidade, possibilitando ataques ou acessos não autorizados.
- **Mitigação:** Ações tomadas para reduzir o impacto ou a probabilidade de exploração de uma vulnerabilidade.
- **Remediação:** Processo de corrigir ou eliminar uma vulnerabilidade identificada, normalmente através de atualizações, *patching* ou reconfiguração.
- **Patch:** Atualização de software destinada a corrigir vulnerabilidades ou melhorar a segurança de sistemas.
- **CVE (Common Vulnerabilities and Exposures):** Sistema de identificação único para vulnerabilidades e exposições de segurança, utilizado globalmente para facilitar o rastreamento e a partilha de informações sobre ameaças.
- **CVSS (Common Vulnerability Scoring System):** Sistema de pontuação utilizado para avaliar a gravidade das vulnerabilidades e priorizar respostas.
- **Scan de Vulnerabilidade:** Processo automatizado de análise de sistemas para identificar possíveis vulnerabilidades.
- **Zero-Day:** Vulnerabilidade não conhecida pelo fabricante ou ainda sem correção disponível, frequentemente explorada em ataques.

