Política de Gestão de Identidades e Acessos da Direção Regional de Informática (DRI)

Ref. Documento:	POLT-004-DRI-Política de Gestão de Identidades e Acessos_v1.0-2026-04-24
Versão:	1.0
Data:	abril de 26
Autor:	DRI
Proprietário	Direção Regional de Informática (DRI)
Classificação:	Pública

Azinhaga do Poço Barral, n.º 23, Edifício Funchal Business Center, piso 1 | 9000-638 Funchal
T. +351 291 145 190 | www.madeira.gov.pt | dri@madeira.gov.pt | NIF: 671 001 310 | NISS: 200 0498 1685

Política de Gestão de Identidades e Acessos da Direção Regional de Informática (DRI)

Revisões - Histórico

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

Tabela 1 – Revisões - Histórico

Aprovação

Nome	Cargo	Assinatura	Data
Dr. César Rosa	Diretor Regional de Informática	CÉSAR MARTIM AGUIAR BAPTISTA ROSA Assinado de forma digital por CÉSAR MARTIM AGUIAR BAPTISTA ROSA Dados: 2026.04.24 16:03:14 +01'00'	

Tabela 2 - Aprovação

Azinhaga do Poço Barral, n.º 23, Edifício Funchal Business Center, piso 1 | 9000-638 Funchal
T. +351 291 145 190 | www.madeira.gov.pt | dri@madeira.gov.pt | NIF: 671 001 310 | NISS: 200 0498 1685

Índice

Azinhaga do Poço Barral, n.º 23, Edifício Funchal Business Center, piso 1 | 9000-638 Funchal
T. +351 291 145 190 | www.madeira.gov.pt | dri@madeira.gov.pt | NIF: 671 001 310 | NISS: 200 0498 1685

1. Introdução

A gestão de identidades e acessos 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, controlar, monitorizar e auditar os acessos aos sistemas e infraestruturas tecnológicas sob responsabilidade da DRI, promovendo um ambiente seguro e resiliente face a ameaças relacionadas com o uso indevido ou não autorizado de identidades. Ao definir procedimentos claros para a gestão de identidades e acessos, 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 identidades e acessos aos sistemas, aplicações e dispositivos sob gestão da DRI sejam controlados de forma eficiente, minimizando riscos para a integridade, disponibilidade e confidencialidade da informação. Para tal, são definidos procedimentos para a criação, atribuição, revisão, revogação e monitorização de identidades e permissões, assegurando que apenas utilizadores autorizados têm acesso aos recursos necessários para o desempenho das suas funções. Esta política visa ainda promover a melhoria contínua dos processos de controlo de acessos, 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 acessos indevidos ou comprometimento de identidades por agentes maliciosos. Ao estabelecer mecanismos robustos de gestão de identidades e acessos, a DRI procura assegurar que as operações críticas permanecem seguras, mesmo perante ameaças emergentes, como ataques de phishing, exploração de credenciais 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 incidentes de acesso, 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 identidades e acessos, 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 identidades e acessos. 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.

Azinhaga do Poço Barral, n.º 23, Edifício Funchal Business Center, piso 1 | 9000-638 Funchal
T. +351 291 145 190 | www.madeira.gov.pt | dri@madeira.gov.pt | NIF: 671 001 310 | NISS: 200 0498 1685

4. Política de Gestão de Identidades e Acessos

A política define que todos os ativos críticos sob gestão da DRI devem ser sujeitos a avaliações periódicas de acessos e identidades, utilizando ferramentas automatizadas, auditorias e revisões de permissões. As identidades e acessos identificados devem ser classificados segundo critérios de risco, priorizados e tratados conforme a gravidade e impacto potencial, com atualização e revogação de acessos, bem como correção de configurações de permissões. A gestão de identidades e acessos 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 identidades e acessos 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 a incidentes de acesso devem respeitar requisitos legais e operacionais, com atualização imediata para acessos críticos e procedimentos definidos para os de menor impacto. O histórico de identidades, acessos e ações tomadas deve ser documentado e revisto periodicamente para garantir a melhoria contínua dos processos de segurança.

5. Responsabilidades

A aplicação desta política de gestão de identidades e acessos exige uma definição clara das responsabilidades de todos os intervenientes, garantindo que os procedimentos sejam cumpridos de forma eficaz e alinhada com as normas internas da DRI.

- Diretor Regional de Informática: aprova a política de gestão de identidades e acessos, assegura a disponibilização de recursos necessários e supervisiona a implementação dos procedimentos definidos, promovendo o alinhamento com os requisitos legais e normativos aplicáveis.
- Responsável de Segurança: coordena as atividades de identificação, avaliação, revisão e revogação de identidades e acessos, monitoriza a execução das ações corretivas e garante a comunicação eficaz das medidas implementadas relativas à gestão de permissões.
- Equipas técnicas: efetuam avaliações periódicas dos acessos e permissões, aplicam correções e atualizações, registam e reportam incidentes identificados, e colaboram na implementação das ações de mitigação, assegurando a conformidade com os procedimentos de gestão de identidades.
- Utilizadores: reportam suspeitas de acessos indevidos ou comprometimento de identidades, garantem que a informação institucional é acedida apenas por quem está autorizado e seguem 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.

Azinhaga do Poço Barral, n.º 23, Edifício Funchal Business Center, piso 1 | 9000-638 Funchal
T. +351 291 145 190 | www.madeira.gov.pt | dri@madeira.gov.pt | NIF: 671 001 310 | NISS: 200 0498 1685

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.

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 e respetiva publicação nos canais de comunicação digitais utilizados pela DRI.

Azinhaga do Poço Barral, n.º 23, Edifício Funchal Business Center, piso 1 | 9000-638 Funchal
T. +351 291 145 190 | www.madeira.gov.pt | dri@madeira.gov.pt | NIF: 671 001 310 | NISS: 200 0498 1685

9. Glossário

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

- **Identidade Digital:** Informação eletrónica que representa um indivíduo, grupo ou entidade, utilizada para autenticação e autorização em sistemas digitais.
- **Autenticação:** Processo de verificação da identidade de um utilizador, normalmente através de credenciais como palavra-passe, biometria ou cartões de acesso.
- **Autorização:** Permissão concedida a um utilizador ou entidade para aceder a recursos ou executar ações específicas dentro de um sistema.
- **Gestão de Identidades:** Conjunto de processos e tecnologias para criar, manter, monitorizar e eliminar identidades digitais, garantindo a segurança e integridade dos acessos.
- **Gestão de Acessos:** Processo de controlo dos direitos de acesso dos utilizadores a sistemas, aplicações e dados, baseado em políticas de segurança definidas pela organização.
- **Single Sign-On (SSO):** Mecanismo que permite ao utilizador aceder a múltiplos sistemas ou aplicações com uma única autenticação, simplificando o processo e melhorando a experiência.
- **Multi-Factor Authentication (MFA):** Sistema de autenticação que exige dois ou mais fatores distintos para validar a identidade do utilizador, aumentando a segurança.
- **Privilegiado:** Utilizador ou conta com permissões superiores, normalmente utilizadas para administração de sistemas ou acesso a dados sensíveis.
- **Direitos de Acesso:** Permissões atribuídas a uma identidade para visualizar, modificar ou gerir recursos em sistemas informáticos.
- **Provisionamento:** Processo de criação e configuração de contas e acessos para novos utilizadores ou entidades em sistemas informáticos.
- **Desprovisionamento:** Remoção ou alteração dos direitos de acesso de utilizadores ou entidades, normalmente quando deixam de necessitar de acesso ou abandonam a organização.
- **Audit Log (Registo de Auditoria):** Registo cronológico das operações realizadas por utilizadores, utilizado para monitorizar e investigar atividades relacionadas com acesso e gestão de identidades.

Azinhaga do Poço Barral, n.º 23, Edifício Funchal Business Center, piso 1 | 9000-638 Funchal
T. +351 291 145 190 | www.madeira.gov.pt | dri@madeira.gov.pt | NIF: 671 001 310 | NISS: 200 0498 1685