



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

Política de Segurança de Informação

DRI-900.20.001-2/2





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

Revisões - Histórico

Versão	Data	Autor da Revisão	Sumário das Alterações
0.1	03-02-2025	Hugo Aguiar	Preparação do documento final para aprovação

Aprovação

Nome	Cargo	Assinatura	Data
Dra. Élia Ribeiro	Diretora Regional de Informática		6/02/25





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

Índice

0. INTRODUÇÃO	4
A DRI	4
Objetivo da Política de Segurança da Informação	4
Âmbito	4
1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	5
Requisitos de Segurança da Informação	5
Estrutura da definição de objetivos	5
Melhoria Contínua da Segurança da Informação	5
Áreas da Política de Segurança da Informação	5
Responsabilidades	6
Aplicação da Política de Segurança da Informação	7





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

0. INTRODUÇÃO

Este documento define a Política de Segurança da Informação da Direção Regional de Informática (DRI).

A DRI

A DRI é um serviço executivo da Secretaria Regional das Finanças, que tem por missão superintender a política regional para a área das tecnologias de informação e comunicação, assim como apoiar a definição das políticas estratégicas da transição digital da Administração Pública Regional e o seu cumprimento, por forma a assegurar a economia, a eficiência, a operacionalidade e a eficácia das tecnologias, sistemas, aplicações e ferramentas informáticas da Administração Pública Regional, garantindo a capacidade formativa e partilha de conhecimento de domínio tecnológico, segurança do seu ciberespaço, a boa gestão dos seus recursos e promover projetos e tecnologias inovadoras de acordo com as orientações e necessidades do Governo Regional

A DRI, em matérias das suas atribuições, pode ainda prestar serviços a outras entidades, nos termos do disposto no artigo 6.º, designadamente de aprovisionamento de material informático ou de consultadoria e suporte técnico.

Objetivo da Política de Segurança da Informação

A segurança da informação tem como principais objetivos garantir os níveis adequados de integridade, autenticidade, disponibilidade e confidencialidade, requeridos para a sua proteção, mitigando assim o impacto de eventuais incidentes que possam comprometer o regular funcionamento da organização.

A integridade consiste na capacidade de prevenir, recuperar e reverter alterações não autorizadas ou acidentais aos dados.

A autenticidade consiste na manutenção da fiabilidade da informação desde o momento da sua produção e ao longo de todo o seu ciclo de vida.

A disponibilidade refere-se à possibilidade de acesso aos dados, quando necessário.

A confidencialidade refere-se à capacidade de proteger os dados daqueles que não estão autorizados a consultá-los, não impedindo o acesso aos mesmos, em tempo útil, de pessoas autorizadas.

Para o cumprimento destes objetivos, a DRI, em conformidade com a legislação e normativos em vigor em matéria de segurança da informação, compromete-se a adotar as melhores práticas nacionais e internacionais e a implementar um conjunto de controlos de segurança da informação para minimizar ao máximo os riscos.

Âmbito

Esta política aplica-se a todos as pessoas, sistemas, processos e procedimentos que constituem os sistemas de informação e redes da DRI, incluindo, funcionários, subcontratantes e terceiros que tenham acesso aos mesmos.

Esta política aplica-se a toda a informação sob a responsabilidade da DRI, independentemente do suporte de registo: eletrónico, papel, ou outro.

Além do acesso adequado à informação necessária para o desempenho das suas funções, todos os utilizadores devem ter conhecimento desta política, sendo-lhes exigido o respeito pelos controlos de segurança implementados.





1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Requisitos de Segurança da Informação

Será acordada e mantida uma definição clara dos requisitos de Segurança da Informação da DRI com todos os utilizadores, de modo que as atividades de segurança da informação estejam focadas no cumprimento dos mesmos.

Poderão vir a ser incluídos requisitos regulamentares e contratuais no processo da segurança da informação.

É um princípio fundamental do programa de segurança da informação da DRI que os controlos implementados sejam orientados às necessidades desta entidade. Neste sentido, serão comunicados de forma regular, a todos os funcionários, através de reuniões e documentos informativos todos os aspetos que promovam a segurança e a proteção de dados pessoais na organização.

Estrutura da definição de objetivos

A definição dos objetivos deverá ser alvo de uma revisão regular. Esses objetivos serão documentados, juntamente com os detalhes de como os mesmos serão alcançados. Estes objetivos devem ser ainda avaliados e acompanhados, como parte do processo de revisão, para garantir que permanecem válidos.

Os procedimentos e controlos de segurança da informação são adotados e alvo de revisão regular à luz do resultado das avaliações de risco e de acordo com o plano de contenção de riscos de segurança da informação.

Melhoria Contínua da Segurança da Informação

Os seguintes pontos estabelecem a Política de Melhoria Contínua da DRI:

- Melhorar continuamente a eficácia dos controlos de segurança da informação;
- Aprimorar os processos e procedimentos atuais para adequá-los às boas práticas, conforme definido em padrões de relevo;
- Aumentar o nível de proatividade em relação à segurança da informação;
- Tornar os processos de controlo da segurança da informação mensuráveis, de maneira a fornecer uma base sólida para decisões informadas;
- Rever as métricas relevantes, com uma periodicidade anual, para avaliar se são necessárias alterações;
- Obter ideias para melhoria contínua podem provir de diversas fontes, incluindo funcionários, utilizadores, subcontratantes, avaliações de risco, relatórios, entre outros. Uma vez identificadas, as ideias serão registadas e analisadas como parte do processo de revisão.

Áreas da Política de Segurança da Informação

A DRI compromete-se a desenvolver políticas e procedimentos específicos que respeitem as normas internacionais de referência, auditáveis, que definem os requisitos para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), abrangendo, nomeadamente as áreas previstas nas normas ISO 27001, ISO 27002.

Neste sentido, a DRI define políticas para uma ampla variedade de áreas relacionadas com a Segurança da Informação que acompanham esta política.

Cada uma destas políticas deve ser definida e aceite por todas as pessoas com competência na área relevante e, quando formalmente aprovada, é comunicada ao público-alvo, dentro e fora da organização, sempre que aplicável.





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

A tabela que se segue apresenta as Políticas de Suporte e resume o conteúdo de cada uma delas e os destinatários das mesmas.

Políticas	Áreas Relacionadas	Destinatários
Política de Utilização Aceitável	Notificação de Incidentes; Desenvolvimento Seguro de Software; Dispositivos Móveis e Bring Your Own Device (BYOD); Hardware e Software; Dispositivos de Armazenamento Removíveis ; Redes Sociais; Comunicação e Correio Eletrónico; Trabalho Remoto; Requisitos de Palavras-Passe	Todos os utilizadores, incluindo terceiros, que utilizam os sistemas de informação geridos pela DRI
Política de Segurança de Rede	Gestão da segurança da rede, redes sem fios, acessos e comunicações de dados e voz.	Todos os utilizadores, incluindo terceiros, que utilizam as redes de comunicações geridos pela DRI.
Política de Gestão de Identidades e Acessos	Registo de utilizadores, gestão de identidades e acessos, revisões de acesso.	Todos os utilizadores, incluindo terceiros, que utilizam os serviços de identidades/acessos geridos pela DRI.
Política de Monitorização e Resposta a Incidentes de Segurança	Monitorização e resposta a incidentes de segurança.	Todos os funcionários envolvidos na monitorização e resposta a incidentes de segurança.
Política de Ciclo de Vida de Desenvolvimento de Serviços Seguros	Desenvolvimento e aquisição de software e serviços. Integração e testes de sistemas	Todos os funcionários envolvidos no desenvolvimento de serviços.

Tabela 1 – Políticas de Suporte

Responsabilidades

Todos os utilizadores estão obrigados a cumprir e a fazer cumprir a presente política de segurança da informação e têm o dever de zelar pela sua proteção e de proceder à comunicação de qualquer evento que provoque, ou possa provocar, uma quebra de segurança da informação.

A Diretora Regional de Informática é responsável pela implementação do Sistema de Gestão da Segurança da Informação da DRI, competindo-lhe aprovar as políticas estabelecidas e fornecer os meios necessários para sua operacionalização.

O Responsável de Segurança é responsável pelas tarefas de implementação, manutenção e operação do sistema, devendo assegurar, designadamente, a gestão de incidentes de segurança, a execução periódica do processo de avaliação dos riscos de segurança, a elaboração dos planos de formação relativos à segurança da informação e a prestação de apoio às equipas técnicas das especialidades integradas nos processos abrangidos pelo sistema.

Os dirigentes dos serviços, devem colaborar com o Responsável de Segurança, na definição, implementação e controlo de aplicação das políticas e procedimentos de segurança que vierem a ser definidos para a sua área de competência e são responsáveis por garantir o seu cumprimento por parte dos recursos humanos e materiais sob sua responsabilidade.





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

Os funcionários devem cumprir e fazer cumprir as políticas, regulamentos e procedimentos relativos à segurança da informação.

Os colaboradores de terceiras entidades que prestam serviço na DRI, ou que utilizam as suas instalações e meios, devem cumprir os normativos e procedimentos estipulados na política de segurança da informação.

Aplicação da Política de Segurança da Informação

O cumprimento das Políticas de Segurança estabelecidas neste documento é obrigatório para todos os processos e procedimentos que compõem os sistemas de informação e redes da DRI. Esta obrigação abrange todos os funcionários da Administração Pública Regional, tanto direta quanto indireta, bem como subcontratantes e terceiros que tenham acesso a esses sistemas e redes.

Cada funcionário, entidade subcontratante e/ou quaisquer terceiros que tenham acesso aos sistemas de informação e redes, é individualmente responsável por conhecer, compreender e cumprir as suas obrigações no que diz respeito à utilização correta e à proteção da informação da DRI.

As violações às políticas de segurança podem resultar em processos disciplinares e, sempre que aplicável, em ações de natureza cível ou penal.

Exceções à presente política deverão ser justificadas previamente através de um processo formal de aceitação de risco.

Qualquer exceção deve ser aprovada antecipadamente, formalmente registada e monitorizada. Todas as ações de monitorização respeitarão rigorosamente a legislação de proteção da privacidade individual.

A Política Geral de Segurança da Informação da DRI será revista anualmente ou sempre que ocorrerem alterações significativas relacionadas com:

1. Legislação e regulamentação aplicável;
2. Estratégias de sistemas de informação;
3. Alteração dos níveis de risco identificados.

Todas as alterações à presente política serão aprovadas pela Direção Regional de Informática e divulgadas a todos os utilizadores.

Dúvidas relacionadas ao âmbito ou à aplicação da presente política devem ser dirigidas à Direção Regional de Informática, através do correio eletrónico: dri@madeira.gov.pt.



