2025

GABINETE REGIONAL PARA A **CONFORMIDADE DIGITAL, PROTEÇÃO DE DADOS** E **CIBERSEGURANÇA**

Região Autónoma da Madeira
Governo Regional

Secretaria Regional das Finanças

Política Geral de Cibersegurança da Administração Pública Regional (APR)

Ref. Documento:	**POLT-001-Ciber-PoliticaGeralAPR_PUB-C1**
Versão:	**1.0**
Data:	**setembro de 2025**
Autor:	**SRF-GCPD**
Proprietário:	**Governo Regional da Madeira (GRM)**
Classificação:	**Pública**

Controlo de versões

Versão	Tipo	Data	Sumário das alterações	Autores
1.0	Versão inicial	27.08.2025	Criação do documento	GCPD

Tabela 1 - Controlo de Versões

Aprovação:

Nome	Cargo	Assinatura	Data
Martin Freitas	Encarregado-Geral de Cibersegurança	Assinado por: **Martin Oliveira de Freitas Freitas** Num. de Identificação: 13368036 Data: 2025.09.08 10:31:36+01'00' Certificado por: **Governo Regional da Madeira** Atributos certificados: **Encarregado-Geral de Cibersegurança da Administração Pública Regional** CHAVE MOVEL	03/09/2025

Tabela 2 - Aprovação

Índice

1 Enquadramento

A crescente digitalização dos serviços públicos da Região Autónoma da Madeira (RAM) tem contribuído para uma maior proximidade com os cidadãos e empresas, oferecendo soluções mais acessíveis, eficientes e modernas. No entanto, esta evolução tecnológica traz consigo novos desafios, entre os quais se destaca a necessidade de garantir elevados níveis de cibersegurança, essenciais para proteger os dados, assegurar a continuidade dos serviços e manter a confiança na relação das partes envolvidas.

Neste contexto, a Administração Pública Regional (APR) da Região Autónoma da Madeira assume o compromisso de adotar medidas robustas de cibersegurança, alinhadas com as melhores práticas internacionais e com os requisitos legais e regulamentares em vigor. Este compromisso visa garantir que os serviços digitais são prestados com segurança, responsabilidade e transparência.

A presente política de cibersegurança reflete este compromisso, orientando-se para a melhoria contínua dos serviços públicos e assegurando a proteção de todos os intervenientes — incluindo cidadãos, empresas, trabalhadores e demais partes interessadas.

Neste âmbito, foi elaborada a presente Política Geral de Cibersegurança da APR, enquadrada no modelo de referência em cibersegurança do Governo Regional da Madeira e alinhada com os requisitos legais decorrentes do Regime Jurídico de Segurnaça do Ciberespaço (RJSC) em vigor, as orientações do Centro Nacional de Cibersegurança (CNCS) e as diretrizes europeias.

2 Âmbito de aplicação

A presente Política Geral de Cibersegurança aplica-se a todos os organismos públicos e trabalhadores da APR, bem como a fornecedores e demais partes interessadas, e qualquer individuo que utilizam os sistemas de informação e serviços digitais sob a responsabilidade da APR. Estão igualmente abrangidos todos os ativos digitais, nomeadamente processos, aplicações, infraestruturas tecnológicas, centros de processamento de dados, localizações físicas e qualquer tipo de dados tratados digitalmente pelas entidades da APR.

3 Destinatários

Esta Política é comunicada a todos os trabalhadores, partes interessadas e ao público em geral.

4 Princípios e fundamentos

A presente política visa garantir os princípios e fundamentos essenciais da cibersegurança, designadamente:

- Princípio da confidencialidade: que assegura que a informação sob a responsabilidade da APR está protegida contra acessos não autorizados;
- Princípio da integridade: que assegura que a informação é precisa e completa, protegendo-a contra alterações não autorizadas, contribuindo para a confiabilidade dos dados e das operações;
- Princípio da disponibilidade: que garante que a informação e os sistemas estão acessíveis quando necessário, mantendo a continuidade das operações e minimizando interrupções;

- Princípio da autenticidade e não-repúdio: que garante que a informação ou identidade é comprovadamente proveniente de origem legítima, sem alteração e que é possível comprovar a autoria ou a entrega de forma segura e auditável;
- Fundamento da governação: os Organismos Regionais comprometem-se em criar mecanismos de governação da cibersegurança eficientes nas suas entidades tendo por base o seu contexto organizacional;
- Fundamento da identificação: os Organismos Regionais compreendem o contexto organizacional para gerir os seus riscos de cibersegurança;
- Fundamento da proteção: os Organismos Regionais implementam medidas/ controlos para assegurar a prestação contínua de serviços de acordo com os requisitos;
- Fundamento da deteção: os Organismos Regionais detêm as capacidades para identificar a ocorrência de eventos de cibersegurança e agir em conformidade;
- Fundamento da resposta: os Organismos Regionais desenvolvem ações para conter o impacto de potenciais incidentes de Cibersegurança;
- Fundamento da recuperação: os Organismos Regionais elaboram e mantém planos para restaurar capacidades ou serviços afetados por incidentes.

5 Objetivos

A Política Geral de Cibersegurança estabelece as diretrizes genéricas para a proteção da confidencialidade, integridade e disponibilidade dos ativos de informação e da infraestrutura TIC (Tecnologias de Informação e Comunicação) da APR, cumpre com os fundamentos da cibersegurança, e promove a conformidade com os requisitos legais e regulamentares das áreas de atividade dos Organismos Regionais, preservando adequadamente os dados e a informação dos organismos, das empresas e dos cidadãos. Assim, através das diretrizes desta política, o Governo Regional da Madeira (GRM) pretende:

- Definir uma abordagem global à cibersegurança para todas as entidades da APR, que seja clara e compreendida da mesma forma pelas diferentes áreas e partes interessadas;
- Fomentar uma cultura de cibersegurança, promovendo a ciber literacia e a sensibilização dos trabalhadores da APR, empresas e cidadãos para a cibersegurança;
- Cumprir e fazer cumprir os requisitos legais e regulamentares a que está obrigado e colaborar com as autoridades nacionais, reguladores e comunidades, em matéria de cibersegurança;
- Proteger os ativos de informação e de TIC dos quais é responsável, de acordo com as melhores práticas preconizadas pelos quadros de referência (*frameworks)* nacionais, europeias e internacionais, promovendo uma cultura baseada no risco, que é considerado desde o início e em todo o sistema, proporcionando uma ação preventiva nas atividades de planeamento, operação, análise e avaliação;
- Focar continuamente na melhoria do sistema de gestão da cibersegurança garantindo a sua adaptação a mudanças internas e externas e potenciando novas oportunidades.

6 Responsabilidades e obrigações

O GRM definiu as funções e responsabilidades relevantes, no contexto da gestão da cibersegurança da APR:

a) Órgãos de Gestão, Direção e Administração

São responsáveis por garantir a implementação da metodologia de gestão de riscos de cibersegurança, o que inclui o cumprimento das medidas de supervisão e de execução, bem como aprovar e assegurar a aplicação das respetivas medidas de tratamento dos riscos de cibersegurança. Compete-lhes ainda promover, de forma regular, ações de formação em cibersegurança, de modo a fortalecer a cultura organizacional e as práticas de gestão dos riscos de Cibersegurança. Adicionalmente, devem garantir a execução do Programa de Cibersegurança transversal definido para a Administração Pública Regional.

b) Gabinete do Encarregado-Geral de Cibersegurança (EGCiber)

O Decreto Regulamentar Regional n.º 10/2024/M, de 14 de fevereiro, determina que, no âmbito do GRM, o GCPD (Gabinete Regional para a Conformidade Digital, Proteção de Dados e Cibersegurança) tem por missão especial assegurar as funções do Encarregado-Geral de Cibersegurança (EGCiber) dos organismos e serviços da administração direta e indireta da Região Autónoma da Madeira e das empresas públicas regionais, incluindo funções de controlo e auditoria em matérias conformidade digital, proteção de dados e cibersegurança. Integra, igualmente, a definição e coordenação do modelo de Programa de Cibersegurança aplicável de forma transversal à Administração Pública Regional.

c) Rede de Cibersegurança

Constitui uma estrutura organizativa destinada à gestão da cibersegurança na Administração Pública da RAM – a Rede de Cibersegurança, coordenada pelo Encarregado Geral de Cibersegurança da APR (EGCiber) – na qual estão incluídos elementos de todas as entidades que tenham serviços de informática próprios, sendo composta pelos seguintes membros:

- Responsável de Cibersegurança da Administração Pública Direta da RAM (DRI - Direção Regional de Informática);
- Responsável de Cibersegurança para as Escolas da RAM (DRE – Direção Regional de Educação);
- Responsável (s) de Cibersegurança por entidade da Administração Indireta e Pública Empresarial (Institutos e EPEs) da RAM;
- Responsável (s) de Cibersegurança das entidades do setor empresarial da RAM.

A Rede de Cibersegurança é responsável pelo acompanhamento, de forma articulada com o GCPD, de todo o processo de implementação do programa de cibersegurança, definição de prioridades e atividades de melhoria contínua, garantindo que os Organismos Regionais estão preparados e resilientes no âmbito da cibersegurança.

d) Responsável de Cibersegurança

É responsável por liderar e acompanhar todas as iniciativas relacionadas com a cibersegurança do seu Organismo, ou grupo de Organismos. O Responsável de Segurança desempenha um papel fundamental na garantia da confidencialidade, integridade e disponibilidade dos ativos relacionados com as redes e sistemas de informação que suportam os processos de negócio do Organismo Regional. Adicionalmente, é também responsável por gerir e monitorizar globalmente as operações de segurança, incluindo monitorização de incidentes de segurança, deteção de ameaças, gestão de vulnerabilidades e gestão de informação e eventos de segurança;

e) Utilizadores / Trabalhadores

São responsáveis pela proteção da informação e pela utilização adequada dos sistemas e recursos tecnológicos, nomeadamente através do reporte de incidentes, anomalias ou comportamentos suspeitos. Para tal, devem conhecer esta Política Geral de Cibersegurança e cumprir as políticas internas específicas e demais procedimentos que lhes sejam comunicados.

f) Terceiros fornecedores de TIC

São responsáveis por cumprir as normas e procedimentos específicos emitidos pelo Organismo Regional, contribuindo para a proteção dos dados e dos sistemas de informação contra acessos não autorizados, perda ou utilização indevida. Devem colaborar no reporte de incidentes, na avaliação de riscos – inclusive em matéria de direitos fundamentais quando estejam em causa tecnologias emergentes e em matéria de proteção de dados – e no cumprimento das medidas definidas para reduzir esses riscos, bem como assegurar a continuidade dos serviços em caso de ocorrências de segurança.

7 Estrutura da Política de Cibersegurança

A Política da Cibersegurança GRM é enquadrada através de um conjunto de regulação em matéria da cibersegurança que a operacionaliza, de acordo com a seguinte estrutura hierárquica:

A **Política Geral**, definida neste documento, estabelece orientações globais para a proteção da informação e dos sistemas de informação da APR, bem como os princípios, os fundamentos, as funções e responsabilidades dos intervenientes.

As **Políticas Internas Específicas** regulam aspetos de proteção inerentes aos diversos domínios da cibersegurança, em conformidade com as atribuições de cada uma das entidades públicas e com as obrigações legais, regulamentares e contratuais aplicáveis. Estabelecem o nível mínimo de segurança e densificam as medidas de segurança de acordo com a realidade de cada entidade, devendo estar sempre alinhadas com a presente política geral. Em caso de eventual incompatibilidade, prevalece a Política Geral.

Em função do âmbito de atuação e atribuições de cada entidade pública, as Políticas Internas Especificas poderão abranger diversos temas concretos, entre os quais se incluem, designadamente:

- Uso Aceitavel (correio eletrónico, equipamentos; redes internas e externas (Wi-Fi), entre outras componentes);
- Classificação da Informação;
- Gestão de risco de cibersegurança;
- Salvaguarda e Recuperação da Informação (Backups&Restore);
- Gestão de Incidentes de Cibersegurança;
- Gestão de Ameaças e Vulnerabilidades;
- Continuidade de Negócio / Recuperação em caso de Desastre;
- Gestão de Ativos;
- Gestão de Identidade e Acessos (IAM);
- Segurança Física e Ambiental;
- Desenvolvimento seguro e de segurança das aplicações;
- Segurança da cadeia de abastecimento;
- Utilização de Dispositivos Móveis (próprios e da organização);
- Segurança da(s) Rede(s);
- Acesso Remoto / Teletrabalho;
- Criptografia e Gestão de Chaves;
- Utilização Segura e Responsável da Inteligência Artificial (IA).

O GCPD poderá desenvolver Políticas Específicas transversais, aplicáveis a todas as entidades públicas, relativamente às temáticas acima referidas ou outras que se afigurem relevantes em matéria de cibersegurança. Esta competência não substitui, contudo, a responsabilidade de cada entidade em definir e implementar as suas próprias políticas, contextualizadas à sua realidade, com base na priorização e gestão dos riscos, respeitando a hierarquia documental definida nesta Política Geral.

Os **Procedimentos, Manuais e Instruções de Trabalho** constituem documentos operacionais que detalham, de forma prática e estruturada, as regras, requisitos e atividades necessários para implementar as Políticas Específicas de Cibersegurança. O seu objetivo é apoiar a execução diária das medidas de segurança, assegurando uniformidade, eficácia, conhecimento organizacional unívoco das etapas a prosseguir e rastreabilidade na aplicação das políticas.

A presente Política Geral de Cibersegurança encontra-se em linha com outras Políticas Gerais já aprovadas na Administração Pública Regional, como a de Privacidade e Proteção de Dados, bem como com quaisquer outras em matérias de conformidade digital, nomeadamente na área da Inteligência Artificial.

Todas as Políticas Gerais partilham o mesmo nível hierárquico documental, complementando-se entre si sem se sobreporem ou colidirem.

8 Gestão de Risco

O **GRM** implementou um quadro de gestão de riscos de segurança da informação, com foco em cibersegurança, que constitui a base para a gestão da cibersegurança da APR e garante um elevado nível de responsabilidade nas medidas adotadas.

Este quadro assenta numa abordagem de **priorização**, orientando todas as intervenções para os riscos com maior impacto potencial na continuidade, segurança e resiliência dos serviços públicos. A identificação, análise e avaliação dos riscos servem de suporte à tomada de decisão, à definição de medidas preventivas e de mitigação e à afetação eficiente de recursos, bem como à delimitação das Políticas Específicas que devem ser definidas caso a caso.

Este instrumento é objeto de revisão regular, em função do contexto situacional, de modo a promover a adaptação face a novas ameaças, vulnerabilidades e a alterações legais e evoluções tecnológicas. Cada entidade pública deve aplicar esse quadro de forma ajustada à sua realidade, em alinhamento com a Política Geral de Cibersegurança da APR.

9 Revisão e atualização

O **GRM** reserva-se o direito de proceder a reajustamentos ou alterações à Política de Geral de cibersegurança e garante a sua revisão periódica.

Esta política foi aprovada em Conselho de Governo Regional, sendo que eventuais revisões que não alterem substancialmente a mesma podem ser apenas divulgadas às partes interessadas.

10 Divulgação e Publicação

Tendo em consideração a classificação pública desta política, este documento será divulgado a todas as partes interessadas através dos canais de comunicação digitais do Governo Regional.