POLÍTICA DE SEGURANÇA DA INFORMAÇÃO(P)

MENAC

MECANISMO NACIONAL ANTICORRUPÇÃO

SGSI

Sistema de Gestão de Segurança da Informação

Aprovo,

Presidente do MENAC

António Pires Henriques da Graça, juiz conselheiro jubilado do STJ

Assinado por: **ANTÓNIO PIRES HENRIQUES DA GRAÇA**
Num. de Identificação:
Data: 2025.02.24 18:57:46+00'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Mecanismo Nacional Anticorrupção**

CARTÃO DE CIDADÃO

Conteúdo

Ficha técnica

Título

SGSI - Política Segurança da Informação (P)

Versão

1.0

Destinatário do documento

Todos os colaboradores do MENAC e as partes interessadas internas e externas que forem consideradas como relevantes.

Classificação da Informação

Pública

Conceção Técnica

Mecanismo Nacional Anticorrupção - UTSI

Responsável pelo SGSI

Eng. João Carlos Mesquitela

Endereço

Escadinhas de São Crispim 7

1100-534

Lisboa

(+351) 21 054 0950

geral@mec-anticorrucao.pt

https://mec-anticorrupcao.pt/

Data de edição

Fevereiro 2025

Siglas e abreviaturas

- **CISO** - Responsável de Cibersegurança
- **CNCS** - Centro Nacional de Cibersegurança
- **DPIA** - Avaliação de Impacto sobre a Proteção de Dados
- **MENAC** - Mecanismo Nacional Anticorrupção
- **QNRCS** - Quadro Nacional de Referência para a Cibersegurança
- **RGPD** - Regulamento Geral de Proteção de Dados
- **SGSI** - Sistema de Gestão de Segurança da Informação
- **SI** - Sistema de Informação

1. INTRODUÇÃO

1.1. OBJETIVO DO DOCUMENTO

O objetivo deste documento é estabelecer a política de segurança da informação, para assegurar que os requisitos de disponibilidade, integridade e confidencialidade da informação gerida pelo Mecanismo Nacional Anticorrupção (MENAC) no âmbito do seu Sistema de Gestão de Segurança da Informação (SGSI), são respondidos adequadamente e alvo de melhoria quando necessário.

1.2. ÂMBITO DE APLICAÇÃO

Esta política é de aplicação obrigatória a todo o âmbito do sistema de gestão de segurança da Informação do MENAC.

1.3. VIGÊNCIA

Qualquer revisão executada sobre este documento, que seja posterior à data da última versão publicada, entrará em vigor imediatamente após a sua publicação, anulando todo e qualquer efeito de versões anteriores.

Se, por motivos técnicos ou funcionais, não for possível aplicar as especificações descritas neste documento, tal facto deverá ser reportado ao Departamento de Serviços e Suporte Tecnológico as alterações necessárias que devem ser realizadas.

1.4. REVISÃO E AVALIAÇÃO

Este documento será avaliado e revisto com uma periodicidade anual ou sempre que necessário.

- Responsabilidade da revisão cabe à UTSI sob supervisão do Secretário-Geral do MENAC;
- Aprovação do documento cabe ao Presidente do MENAC

1.5. DOCUMENTOS DE REFERÊNCIA

Para a realização deste documento, são tidas como referências as seguintes fontes:

- ISO/IEC 27001:2022 - Sistema de Gestão da Segurança da Informação: 5.2;
- ISO/IEC 27002:2022 - Código de Boas Práticas para a Gestão da Segurança da Informação;
- Política e Normas de Segurança do MENAC;
- Decretos de Lei e outras legislações aplicáveis.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A proteção no acesso, tratamento, salvaguarda e transmissão de informação, em consonância com os requisitos profissionais, éticos, legais, regulamentares e contratuais, constitui uma das mais altas prioridades do MENAC e é considerada fundamental para o seu sucesso.

A perda ou o roubo de informação pode resultar em consequências severas a nível legal, financeiro e reputacional, pelo que o MENAC se compromete a salvaguardar a confidencialidade, integridade e disponibilidade de toda a informação sob a sua custódia, seja ela em suporte físico, digital ou intelectual.

O MENAC implementou e mantém um Sistema de Gestão de Segurança da Informação (SGSI), composto por políticas, processos e procedimentos concebidos para preservar, monitorizar e aperfeiçoar a segurança da informação, com base numa rigorosa avaliação dos riscos existentes.

A Política de Segurança da Informação do MENAC fundamenta-se na adaptação de normas internacionais recomendadas, como a ISO 27001:2022, que estabelece princípios gerais aplicáveis à segurança da informação e aos ativos de suporte (servidores, sistemas de informação, redes, infraestruturas, entre outros), no âmbito do SGSI, respeitando a legislação e regulamentação aplicáveis.

O incumprimento das políticas, processos e procedimentos do SGSI, que resulte em interrupções de serviço, fuga ou roubo de informação para entidades não autorizadas, ou modificação indevida da informação, pode ter

consequências significativas a nível financeiro, jurídico e reputacional, além de afetar a confiança das partes interessadas.

É da responsabilidade de todas as partes envolvidas contribuir ativamente para a proteção e segurança da informação.

2.1. PRINCÍPIOS

A política de segurança da informação do MENAC, visa garantir os seguintes princípios:

1. A informação está protegida contra acessos não autorizados;
2. A confidencialidade da informação está garantida;
3. A integridade da informação é mantida;
4. Todas as leis e regulamentos aplicáveis são respeitados;
5. Os planos de continuidade de negócio apropriados são mantidos e testados regularmente;
6. Todas as quebras de segurança da informação detetadas ou sob suspeita, são investigadas pelas áreas com competência para o efeito.

2.2. OBJETIVOS

Constituem-se como principais objetivos do SGSI:

- Garantir que todos os colaboradores têm conhecimento e cumprem as políticas e
- procedimentos de segurança existentes;
- Definir e comunicar responsabilidades ao nível da Segurança de Informação no âmbito do SGSI;
- Promover a consciencialização contínua sobre a segurança de informação e realizar programas de formação para garantir que todos os colaboradores compreendem a forma como a segurança de informação faz parte das suas funções e as responsabilidades que têm na proteção da confidencialidade, integridade e disponibilidade da informação;
- Incluir a segurança de informação como componente essencial de todos os aspetos de planeamento e operações do MENAC;
- Identificar as principais áreas de risco inerentes à atividade da segurança da informação, avaliando continuamente as ameaças de segurança de

informação, garantindo que estas são identificadas e geridas tendo por base a avaliação de risco e a aplicação de medidas adequadas;

- Promover a proteção adequada da infraestrutura de sistemas de informação e comunicações contra perda, má utilização ou acessos indevidos;
- Estabelecer o acesso à informação somente a pessoas a autorizadas para o exercício das suas funções;
- Estabelecer os princípios e regras de segurança inerentes aos recursos de informática;
- Promover a deteção, registo, reporte e investigação de incidentes de segurança de forma eficaz e eficiente para garantir a minimização dos impactos deste tipo de incidentes;
- Promover requisitos de segurança da informação a considerar na gestão da continuidade das operações de negócio.
- Garantir a disponibilização dos recursos necessários para a efetiva manutenção e melhoria contínua do SGSI;
- Promover a revisão contínua dos mecanismos e processos de segurança para assegurar que são efetivos, relevantes e adequados às necessidades.

2.3. RESPONSABILIDADES

O Presidente do MENAC é responsável por manter a presente Política de Cibersegurança atualizada e assegurar a sua execução, garantindo os meios técnicos e financeiros necessários para o cumprimento dos objetivos estabelecidos.

No âmbito das atribuições conferidas, a Unidade de Tecnologias e Sistemas de Informação (UTSI) poderá propor ao Secretário-Geral, para aprovação, alterações à presente política e aos documentos e estratégias implementados no domínio da Cibersegurança.

Após a aprovação do Secretário-Geral, as propostas podem ser submetidas ao Presidente do MENAC para deliberação final.

Compete ao Presidente do MENAC:

- Nomear um ponto de contacto permanente com o Centro Nacional de Cibersegurança (CNCS);
- Designar um responsável pela (Ciber)segurança (CISO).

O MENAC deve comunicar ao CNCS, no prazo de 20 dias úteis, a identidade do ponto de contacto permanente e do responsável pela (Ciber)segurança (CISO).

No exercício das suas funções, o CISO deverá:

1. Garantir a implementação de boas práticas de segurança que preservem a integridade, confidencialidade e disponibilidade das informações e dos sistemas do MENAC;
2. Promover ações de formação e sensibilização em cibersegurança;
3. Desenvolver políticas e procedimentos de segurança da informação e cibersegurança;
4. Elaborar um Plano de Segurança;
5. Participar ativamente na gestão de incidentes;
6. Assegurar a gestão de riscos de cibersegurança;
7. Avaliar o desempenho de todos os procedimentos de segurança da informação e de cibersegurança implementados, propondo medidas de melhoria;
8. Redigir um relatório anual, em conformidade com o disposto no artigo 8.º do Decreto-Lei n.º 65/2021, de 30 de julho.

O ponto de contacto permanente deverá assegurar, a nível operacional e técnico, os fluxos de informação previstos no artigo 4.º do Decreto-Lei n.º 65/2021, de 30 de julho, com o CNCS.

3. RECOMENDAÇÕES DE SEGURANÇA

Todos os colaboradores do MENAC são responsáveis pela proteção dos ativos da organização, devendo, no âmbito das suas funções, conhecer as suas responsabilidades na mitigação de riscos de segurança, zelando pela integridade, confidencialidade e disponibilidade da informação e sistemas do MENAC.

3.1. Responsabilidades de Cibersegurança

1. Os colaboradores são responsáveis pela proteção e uso adequado dos equipamentos informáticos que lhe são atribuídos pelo MENAC, devendo estes ser utilizados exclusivamente para fins profissionais;
2. Todas as senhas utilizadas devem ter um mínimo de 12 caracteres, incluindo uma combinação de letras maiúsculas, minúsculas, números e símbolos. É

imperativo que cada senha seja única e não reutilizada em diversas contas ou serviços. A política exige a alteração das senhas a cada 90 dias, sem repetir as últimas cinco utilizadas. A partilha de senhas é proibida, assim como a sua anotação em locais inseguros. Recomenda-se vivamente a utilização da autenticação vários fatores (no mínimo dois), sempre que disponível, para reforçar a segurança. Em caso de suspeita de comprometimento de uma senha, o utilizador deve proceder à sua imediata alteração e reportar o incidente à equipa de segurança da informação.

3. É obrigatório o uso de VPN no acesso aos SI fora das instalações do MENAC;
4. Aquando do exercício das suas funções em teletrabalho, é expressamente proibido aos trabalhadores do MENAC o uso de redes WI-FI públicas (redes WI-FI de cafés, centros comerciais e outros lugares que representem um elevado risco de Cibersegurança);
5. Em caso de receção de e-mail fraudulento o colaborador não deve abrir qualquer ficheiro anexo ao mesmo, deverá, no entanto, enviar o e-mail fraudulento como anexo para o endereço de correio eletrónico informatica@mec-anticorrupcao.pt;
6. As falhas no funcionamento dos SI ou suspeita de vírus/malware devem ser comunicadas à UTSI, através do email informatica@mec-anticorrupcao.pt;
7. É expressamente proibido o acesso a sites da Internet ou o download de ficheiros que possam colocar em causa a integridade da infraestrutura tecnológica, devendo, em caso de dúvida, contactar-se a equipa de suporte da UTSI para aferir a existência de risco de segurança.

3.2. PROTEÇÃO DE DADOS PESSOAIS

3.2.1. Objetivo

O MENAC, enquanto responsável pelo tratamento de dados pessoais, estabelece nesta secção as práticas e medidas de proteção de dados pessoais, com o objetivo de garantir conformidade com o Regulamento Geral de Proteção de Dados (RGPD) e demais legislações aplicáveis.

Esta política visa proteger os dados pessoais tratados pelo MENAC, promovendo a privacidade e a confiança dos titulares de dados.

3.2.2. Princípios de Proteção de Dados

Para assegurar uma gestão responsável dos dados pessoais, o MENAC adota os seguintes princípios:

i. **Licitude, Lealdade e Transparência**: O tratamento de dados pessoais pelo MENAC é realizado de forma lícita, justa e transparente. Os titulares são informados da finalidade do tratamento e das suas opções de consentimento.

ii. **Limitação das Finalidades**: Os dados pessoais são tratados exclusivamente para fins específicos, explícitos e legítimos, alinhados com as atribuições do MENAC, e não serão usados para outros fins sem o consentimento explícito dos titulares.

iii. **Minimização dos Dados**: O MENAC compromete-se a recolher e tratar apenas os dados pessoais estritamente necessários para a realização dos seus objetivos institucionais.

iv. **Exatidão e Atualização**: O MENAC toma medidas para garantir a exatidão dos dados pessoais, corrigindo e atualizando-os sempre que necessário.

v. **Limitação da Conservação**: Os dados pessoais são mantidos apenas pelo tempo necessário para o cumprimento da finalidade do tratamento, conforme as políticas de retenção de dados do MENAC.

vi. **Integridade e Confidencialidade**: O MENAC implementa medidas técnicas e organizativas apropriadas para proteger os dados pessoais contra acessos não autorizados, perda ou destruição.

3.2.3. Direitos dos Titulares dos Dados

O MENAC assegura que todos os titulares de dados pessoais possam exercer os seus direitos, conforme previsto no RGPD:

- **Direito de Acesso**: Os titulares têm o direito de solicitar informações sobre os dados pessoais tratados pelo MENAC e obter uma cópia dos mesmos.

- **Direito à Retificação e à Eliminação**: Os titulares podem solicitar a correção de dados incorretos ou a eliminação dos dados pessoais, salvo em situações onde exista uma exigência legal de retenção.

- **Direito à Limitação e à Oposição**: É garantido o direito de solicitar a limitação ou se opor ao tratamento dos seus dados pessoais em determinadas situações.

- **Direito à Portabilidade**: Quando aplicável, o MENAC assegura a portabilidade dos dados, permitindo aos titulares transferirem os seus dados para outra entidade.

- **Direito de Retirar o Consentimento**: Quando o tratamento se baseia no consentimento, os titulares podem retirá-lo a qualquer momento, sem comprometer a legalidade do tratamento previamente realizado.

3.2.4. Medidas Técnicas e Organizativas de Segurança

O MENAC adota as seguintes medidas de segurança para proteger os dados pessoais:

- **Controlo de Acessos**: O acesso aos dados pessoais é restrito aos colaboradores cujas funções exigem o manuseio dessas informações, conforme o princípio do menor privilégio.

- **Pseudonimização e Encriptação**: Sempre que possível, o MENAC aplica pseudonimização e encriptação aos dados pessoais para mitigar os riscos em caso de acessos não autorizados.

- **Registo de Atividades de Tratamento**: O MENAC mantém um registo atualizado das atividades de tratamento de dados pessoais, em conformidade com o RGPD.

- **Avaliação de Impacto sobre a Proteção de Dados (DPIA)**: Antes de iniciar novos processos de tratamento que possam representar alto risco aos direitos dos titulares, o MENAC realiza uma DPIA para identificar e mitigar riscos.

4. **Impressoras e documentos físicos**:

    - As impressoras devem ser configuradas com controlo de acesso lógico. Na ausência deste, devem estar em locais reservados e seguros.

    - Os documentos impressos devem ser recolhidos imediatamente após a impressão, evitando que sejam deixados em impressoras, mesas, faxes ou fotocopiadoras.

    - Sempre que documentos físicos não estiverem em uso, devem ser armazenados de forma segura, protegendo-os contra acessos não autorizados.

5. **Destruição de documentos e informação sensível**:

    - Todos os documentos classificados como sensíveis devem ser destruídos de acordo com os procedimentos internos e as normas aplicáveis, garantindo a eliminação segura.

6. **Gestão de palavras-passe**:

    - As palavras-passe devem cumprir os requisitos definidos na política de segurança do MENAC. É proibido anotá-las em suportes físicos ou partilhá-las com terceiros.

7. **Segurança de objetos de acesso**:

    - Chaves e cartões de acesso não devem ser deixados sem supervisão e devem ser mantidos em local seguro.

8. **Limpeza de superfícies de trabalho e ferramentas colaborativas**:

    - Quadros de reuniões e flip charts devem ser apagados após a utilização, garantindo que não contenham informações sensíveis acessíveis a terceiros.

9. **Conferências e comunicações confidenciais**:

    - Informações confidenciais não devem ser discutidas em "open spaces" ou áreas públicas. Sempre que necessário, devem ser