| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insira aqui a designação da entidade jurídica registada | | | | | | | |
| Número do documento:<br>P06S | | | | | Título do documento:<br>**Política de Gestão de Riscos** | | | | | | | |
| Versão:<br>1.0 | | Data de entrada em vigor:<br>01.01.2025 | | | Proprietário do documento: | | | | | | | |
| X | Política | | Norma | | Procedimento | | Formulário | | Registo | | Outro | |

| **Histórico de revisões** | | | | |
|---|---|---|---|---|
| **Número da revisão** | **Data da revisão** | **Alterações** | **Revisto por** | **Proprietário do processo** |
| | | | | |
| | | | | |

| **Aprovações** | | | |
|---|---|---|---|
| **Nome** | **Cargo** | **Data** | **Assinatura** |
| | | | |
| | | | |

Alinhamento com normas e regulamentos aplicáveis

| Norma/Regulamento | Cláusula/Artigo | Comentário |
|---|---|---|
| ISO/IEC 27001:2022 | Cláusulas 6.1, 6.1.3 | |
| ISO/IEC 27002:2022 | 5.4, 5.25 | |
| NIST SP 800-53 Rev. 5 | RA-1 a RA-7, PM-9 | |
| Diretiva NIS2 da UE | Artigo 21(2)(a–d) | |
| DORA da UE | Artigo 5 | |
| COBIT 2019 | APO12, MEA | |

**1. Finalidade**

1.1 A presente política define a forma como a organização identifica, avalia e gere os riscos relacionados com a segurança da informação, as operações, a tecnologia e os serviços prestados por terceiros.

1.2 Assegura que a gestão de riscos constitui parte integrante do planeamento, da execução de projetos, da seleção de fornecedores e da resposta a incidentes, em alinhamento com a ISO 27001, a ISO 31000 e os requisitos regulamentares aplicáveis.

1.3 A política apoia a tomada de decisão informada, a proteção dos ativos de informação e a resiliência das operações críticas do negócio.

**2. Âmbito**

**2.1 A presente política aplica-se a:**

2.1.1 Todos os departamentos, sistemas e utilizadores da organização.

2.1.2 Toda a informação, serviços e ativos geridos internamente ou através de terceiros.

2.1.3 Atividades relacionadas com risco, incluindo revisões de projetos, atualizações de sistemas, externalização e cumprimento regulamentar.

**2.2 Inclui todos os tipos de risco, tais como:**

2.2.1 Ameaças de cibersegurança e vulnerabilidades de sistemas.

2.2.2 Interrupções operacionais e indisponibilidade de serviços.

2.2.3 Exposição legal, de conformidade ou reputacional.

2.2.4 Riscos de terceiros e da cadeia de abastecimento.

2.3 Todos os trabalhadores e prestadores de serviços devem cumprir esta política ao identificar ou comunicar riscos.

**3. Objetivos**

3.1 Integrar procedimentos de avaliação de risco simples e repetíveis nas operações correntes do negócio.

3.2 Identificar e priorizar riscos que possam afetar a Confidencialidade, Integridade e Disponibilidade da informação ou o cumprimento de obrigações legais.

3.3 Atribuir a titularidade do risco e definir ações de tratamento para todos os riscos significativos.

3.4 Manter um registo de riscos rigoroso e atualizado para suportar a demonstração de conformidade em auditoria e o acompanhamento do estado dos riscos.

3.5 Assegurar o envolvimento da gestão na aprovação da tolerância ao risco e dos principais planos de tratamento.

## 4. Papéis e responsabilidades

### 4.1 Diretor-Geral (GM)

4.1.1 Define o apetite pelo risco da organização e aprova o quadro de gestão de riscos.

4.1.2 Aprova as principais decisões de tratamento de riscos e os recursos associados.

4.1.3 Revê trimestralmente os principais riscos com o Coordenador de Risco.

### 4.2 Coordenador de Risco (ou responsável pelo SGSI)

4.2.1 Facilita as avaliações de risco e mantém o registo de riscos.

4.2.2 Assegura que a classificação do risco, a titularidade do risco e as ações de tratamento se encontram documentadas.

4.2.3 Organiza, pelo menos, uma revisão formal de risco por ano.

[ ... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ... ]

## 9. Requisitos de revisão e atualização

### 9.1 Revisão anual da política

9.1.1 Esta política deve ser revista pelo menos uma vez por ano pelo Diretor-Geral (GM) e pelo Coordenador de Risco, para assegurar a sua relevância e integralidade.

### 9.2 Fatores desencadeadores de atualização

#### 9.2.1 Deve ocorrer uma revisão e atualização antecipadas se:

9.2.1.1 Um incidente grave ou uma constatação de auditoria expuser lacunas de controlo relacionadas com risco.

9.2.1.2 Forem introduzidas novas unidades de negócio, tecnologias ou parcerias.

9.2.1.3 Ocorrer alteração de um requisito regulamentar ou contratual.

### 9.3 Controlo de versões

#### 9.3.1 Todas as atualizações desta política devem estar sujeitas a controlo de versões com os seguintes metadados:

9.3.1.1 Número da versão e data de entrada em vigor.

9.3.1.2 Resumo das alterações.

9.3.1.3 Aprovador (Diretor-Geral (GM)).

9.3.1.4 Versões anteriores arquivadas para efeitos de auditoria.

### 9.4 Comunicação e sensibilização

9.4.1 As versões atualizadas da política e os principais planos de tratamento de riscos devem ser comunicados ao pessoal afetado. A formação anual de sensibilização deve incluir princípios fundamentais de sensibilização para o risco.

## 10. Políticas relacionadas e articulações

### 10.1 Esta política articula-se com várias outras para assegurar uma governação da segurança abrangente:

10.1.1 P2S – Política de Papéis e Responsabilidades de Governação: define quem é responsável pela titularidade do risco e pela tomada de decisão.

10.1.2 P5S – Política de Gestão de Alterações: exige a avaliação de riscos antes da implementação de alterações técnicas ou processuais.

10.1.3 P17S – Política de Proteção de Dados e Privacidade: trata o risco regulamentar associado ao tratamento de dados pessoais.

10.1.4 P30S – Política de Resposta a Incidentes (P30): assegura que o tratamento de riscos prossegue durante e após incidentes de segurança.

10.1.5 P33S – Política de Continuidade do Negócio: identifica riscos residuais e medidas de recuperação para serviços críticos.

## 11. Normas e referenciais aplicáveis

### 11.1 ISO/IEC 27001:

11.1.1 Cláusula 6.1 – Estabelece um processo formal de gestão de riscos e de planeamento do tratamento.

11.1.2 Cláusula 6.1.3 – Exige que as organizações mantenham planos de tratamento documentados e as correspondentes aprovações.

### 11.2 ISO/IEC 27002:

11.2.1 Controlos 5.4, 5.25 – Fornecem orientações de implementação para a titularidade do risco, a priorização e a gestão do ciclo de vida.

### 11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 a RA-7 – Definem avaliação de riscos, estratégias de resposta, documentação e mecanismos de revisão.

11.4 PM-9 – Exige supervisão consistente, ao nível da gestão, dos riscos organizacionais.

### 11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(a–d) – Impõe controlos obrigatórios de avaliação de riscos, mitigação e governação às entidades essenciais e importantes.

### 11.6 DORA da UE

11.6.1 Artigo 5 – Exige que as entidades reguladas definam e gerem quadros de gestão do risco das TIC, incluindo identificação, classificação e resposta.

### 11.7 COBIT 2019

11.7.1 APO12 – Gerir Risco: integra o risco no planeamento estratégico e operacional.

11.7.2 MEA01 – Monitorizar, Avaliar e Analisar: assegura a eficácia e a conformidade dos processos e das ações de risco.