Política de gestão de riscos

*Objeto**: Política de gestão dos riscos**Data**: [Inserir data]**Responsável**: CISO, equipa de gestão dos riscos, quadros superiores

A presente política de gestão de riscos é desenvolvida em conformidade com o n.º 2, ponto A, do artigo 21.º da Diretiva NIS2. O objetivo do documento é fornecer um quadro para identificar, avaliar e gerir os riscos de segurança da informação, protegendo a integridade e a disponibilidade dos dados da empresa.

1. Objetivo da política

O objetivo desta política é garantir que a organização adopte uma abordagem estruturada e sistemática da gestão dos riscos, a fim de minimizar o impacto das ameaças à cibersegurança e assegurar a continuidade das actividades.

2. Âmbito de aplicação

Esta política aplica-se a todos os funcionários, prestadores de serviços e terceiros que acedem, gerem ou processam os recursos e dados informáticos da organização.

3. Princípios da gestão de riscos

organização deve adotar os seguintes princípios de gestão do risco:1. **Identificação do risco**: Identificar os riscos de segurança da informação em todas as actividades da empresa.
2. **Avaliação do risco**: Avaliar o impacto e a probabilidade dos riscos identificados, utilizando uma escala de risco.
3. **Tratamento do risco**: Implementar controlos e medidas para mitigar ou eliminar os

riscos identificados.
4. **Monitorização e revisão**: Monitorizar continuamente os riscos e rever periodicamente as medidas tomadas.

4. Avaliação dos riscos

A organização deve efetuar avaliações de risco regulares para identificar ameaças emergentes e avaliar a eficácia dos controlos de segurança existentes.
s avaliações devem considerar:- Riscos de segurança da informação.
- Riscos operacionais.
- Riscos jurídicos e de conformidade

5. Gestão do risco residual

Após a aplicação das medidas de atenuação, a organização deve identificar e aceitar formalmente os riscos residuais. Estes riscos devem ser geridos através de planos de continuidade da atividade e revistos periodicamente.

6. Acompanhamento e revisão das políticas

A política de gestão de riscos deve ser revista e actualizada periodicamente para garantir que está alinhada com os objectivos empresariais e com as alterações no panorama das ameaças.