Política de Gestão de Riscos Cibernéticos para Empresas Financeiras

Baseada no Framework NIST 800-53

2. Propósito

Estabelecer um processo formal para identificar, avaliar e mitigar os riscos cibernéticos que podem afetar a confidencialidade, integridade e disponibilidade dos dados e sistemas da empresa.

3. Escopo

Aplica-se a todos os recursos de informação e tecnologia da empresa, incluindo:

- **Sistemas:** computadores, softwares, redes, etc.
- **Dados:** informações confidenciais, financeiras e de clientes.
- **Processos:** atividades relacionadas à coleta, armazenamento, processamento e transmissão de dados.

4. Política

4.1. Identificação de Riscos

A empresa realizará periodicamente uma avaliação de riscos para identificar os principais riscos cibernéticos que podem afetar seus recursos de informação e tecnologia.

4.2. Análise de Riscos

A empresa analisará os riscos identificados para determinar sua probabilidade de ocorrência e impacto potencial.

4.3. Mitigação de Riscos

A empresa implementará medidas de controle para mitigar os riscos cibernéticos identificados, como:

- **Controles técnicos:** firewalls, antivírus, criptografia, etc.
- **Controles administrativos:** políticas de segurança, treinamentos, etc.
- **Controles físicos:** controle de acesso, segurança ambiental, etc.

4.4. Monitoramento e Revisão

A empresa monitorará continuamente os riscos cibernéticos e revisará periodicamente sua estratégia de gestão de riscos para garantir sua efetividade.

5. Procedimentos Relacionados

- Política de Segurança da Informação
- Política de Controle de Acesso
- Política de Autenticação

6. Não Conformidade

O não cumprimento desta política pode resultar em sanções disciplinares, incluindo:

- Advertência verbal
- Advertência por escrito
- Suspensão do acesso aos recursos de informação e tecnologia
- Rescisão do contrato de trabalho
- Processo judicial, em caso de danos à empresa ou a terceiros.

7. Compromisso/Autoridade da Gestão

A alta administração da empresa está comprometida com a segurança da informação e com a proteção dos dados. A equipe de TI

é responsável pela implementação e monitoramento desta política.

8. Cronograma de Revisão

Esta política será revisada anualmente ou quando necessário.

9. Definições

- **Risco cibernético:** possibilidade de um evento que possa causar danos aos recursos de informação e tecnologia da empresa.
- **Gestão de riscos cibernéticos:** processo de identificar, avaliar e mitigar os riscos cibernéticos.
- **Controle de segurança:** medida para prevenir, detectar e corrigir falhas de segurança.

Observações:

- Esta política é um exemplo e pode ser adaptada às necessidades específicas da empresa.
- É importante consultar especialistas em segurança da informação para auxiliar na implementação da política.