



Política de segurança da informação

MATRIZ DE RISCO





Sumário

1. Objetivo.....	3
2. Critérios de Avaliação	3
3. Lista de Riscos Identificados.....	4
4. Classificação do Nível de Risco	5
5. Controle de alterações.....	6



1. Objetivo

Estabelecer uma visão estruturada dos principais riscos relacionados à segurança da informação, permitindo seu monitoramento contínuo, priorização de ações e planejamento de contingências, conforme os critérios de probabilidade e impacto.

2. Critérios de Avaliação

Nível 1

- Probabilidade: Raro – Pouco provável
- Impacto: Baixo – Impacto operacional leve

Nível 2

- Probabilidade: Possível – Pode ocorrer
- Impacto: Moderado – Prejuízo financeiro ou à reputação

Nível 3

- Probabilidade: Provável – Ocorre com frequência
- Impacto: Alto – Perda de dados, parada crítica ou sanções legais

Cálculo de Risco = Probabilidade x Impacto



3. Lista de Riscos Identificados

R01 – Vazamento de dados em ferramenta de compartilhamento na nuvem

- Categoria: Confidencialidade
- Probabilidade: 2
- Impacto: 3
- Risco: 6
- Ação de mitigação: Revisão de permissões, MFA e criptografia
- Responsável: TI
- Status: Em andamento

R02 – Colaborador remoto acessa dados em Wi-Fi inseguro

- Categoria: Confidencialidade
- Probabilidade: 2
- Impacto: 2
- Risco: 4
- Ação de mitigação: Política de VPN obrigatória e orientação sobre redes públicas
- Responsável: Segurança da Informação
- Status: Em execução

R03 – Perda de acesso ao servidor em colocation por falha de energia

- Categoria: Disponibilidade
- Probabilidade: 1
- Impacto: 3
- Risco: 3
- Ação de mitigação: UPS local + backup em nuvem (OneDrive/SharePoint)
- Responsável: Infraestrutura
- Status: Concluído

R04 – Acesso indevido após desligamento de colaborador

- Categoria: Controle de Acesso
- Probabilidade: 3



- Impacto: 2
- Risco: 6
- Ação de mitigação: Processo de revogação imediata de credenciais
- Responsável: RH + TI
- Status: Em execução

R05 – Ransomware via phishing

- Categoria: Integridade / Continuidade
- Probabilidade: 2
- Impacto: 3
- Risco: 6
- Ação de mitigação: Antivírus, backup recorrente e campanha de conscientização
- Responsável: TI / Comunicação Interna
- Status: Planejado

R06 – Perda de documentos por exclusão indevida

- Categoria: Integridade / Continuidade
- Probabilidade: 2
- Impacto: 2
- Risco: 4
- Ação de mitigação: Política de versionamento no OneDrive + treinamento
- Responsável: Todos os Colaboradores
- Status: Em andamento

4. Classificação do Nível de Risco

1 a 2: Baixo

3 a 4: Moderado

6 a 9: Alto





5. Controle de alterações

Versão	Data	Quem	Anotações
2	04/02/2025	Luis Bartolomei	Aprovação
1	03/12/2024	Thiago Ramiro	Criação

