Política de Gestão de Riscos Cibernéticos para Empresas de Telecomunicações

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, sistemas e infraestrutura da empresa de telecomunicações, considerando as características específicas do setor.

3. Escopo

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

- **Sistemas:** computadores, softwares, redes, sistemas de telecomunicações, etc.
- **Dados:** informações confidenciais, financeiras, de clientes e de tráfego de telecomunicações.
- **Processos:** atividades relacionadas à coleta, armazenamento, processamento e transmissão de dados.
- **Infraestrutura:** torres de celular, cabos de fibra óptica, data centers, etc.

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, infraestrutura e dados, de acordo com as características específicas do setor de telecomunicações, como:

- **Ataques à infraestrutura:** sabotagem física de torres de celular ou cabos de fibra óptica.
- **Interceptação de dados:** roubo de informações confidenciais ou de tráfego de telecomunicações.
- **Ataques de negação de serviço:** interrupção dos serviços de telecomunicações.
- **Falhas de segurança em software:** vulnerabilidades em softwares utilizados em sistemas de telecomunicações.
- **Violações de dados:** acesso não autorizado a dados confidenciais ou de clientes.

4.2. Análise de Riscos

A empresa analisará os riscos identificados para determinar sua probabilidade de ocorrência e impacto potencial, considerando os impactos específicos no setor de telecomunicações, como:

- **Impacto financeiro:** perda de receita, custos de recuperação de dados, etc.
- **Impacto na reputação:** perda de confiança dos clientes, danos à imagem da empresa.
- **Impacto na qualidade dos serviços:** interrupção dos serviços de telecomunicações, degradação da qualidade do serviço.
- **Impacto legal:** sanções por violações de leis e regulamentações.

4.3. Mitigação de Riscos

A empresa implementará medidas de controle para mitigar os riscos cibernéticos identificados, considerando as melhores práticas para o setor de telecomunicações, como:

- **Controles técnicos:** firewalls, antivírus, criptografia, sistemas de detecção de intrusão (IDS), sistemas de prevenção de intrusão (IPS), etc.
- **Controles administrativos:** políticas de segurança, treinamentos, planos de resposta a incidentes, etc.
- **Controles físicos:** controle de acesso, segurança ambiental, monitoramento físico da infraestrutura, etc.
- **Controles específicos para o setor de telecomunicações:** medidas de segurança para redes de telecomunicações, sistemas de billing, 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, considerando as mudanças no setor de telecomunicações e as novas ameaças cibernéticas.

5. Procedimentos Relacionados

- Política de Segurança da Informação
- Política de Controle de Acesso
- Política de Autenticação
- Plano de Resposta a Incidentes

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, com a proteção dos dados e com a segurança da infraestrutura de telecomunicações. A equipe de TI, em conjunto com a equipe de segurança de telecomunicações, é responsável pela implementação e monitoramento desta política.

8. Cronograma de Revisão

Esta política será revisada anualmente ou quando necessário, especialmente em resposta a mudanças no setor de telecomunicações ou novas ameaças cibernéticas.

9. Definições

- **Risco cibernético:** possibilidade de um evento que possa causar danos aos recursos de informação e tecnologia, infraestrutura e dados da empresa de