Política de Análise de Vulnerabilidades para Empresas de Telecomunicações

Baseada no Framework NIST 800-53

2. Propósito

Estabelecer um processo formal para identificar, analisar e corrigir vulnerabilidades em sistemas de informação e tecnologia, infraestrutura e dados da empresa de telecomunicações, com o objetivo de garantir a confidencialidade, integridade e disponibilidade dos recursos de informação e proteger a empresa contra ataques cibernéticos.

3. Escopo

Aplica-se a todos os sistemas 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.
- **Infraestrutura:** torres de celular, cabos de fibra óptica, data centers, etc.

4. Política

4.1. Identificação de Vulnerabilidades

A empresa realizará periodicamente análises de vulnerabilidades em seus sistemas de informação e tecnologia, infraestrutura e dados, utilizando ferramentas automatizadas e manuais, como:

- **Scanners de vulnerabilidades:** ferramentas automatizadas que identificam vulnerabilidades conhecidas em sistemas e softwares.
- **Testes de penetração:** simulações de ataques cibernéticos para identificar vulnerabilidades que podem ser exploradas por atacantes.
- **Análise de código-fonte:** revisão do código-fonte de softwares para identificar vulnerabilidades de segurança.

4.2. Análise de Vulnerabilidades

A empresa analisará as vulnerabilidades identificadas para determinar sua severidade e potencial de exploração, considerando os seguintes fatores:

- **Tipo de vulnerabilidade:** tipo de falha de segurança que pode ser explorada por atacantes.
- **Severidade da vulnerabilidade:** impacto potencial da exploração da vulnerabilidade.
- **Facilidade de exploração:** facilidade com que a vulnerabilidade pode ser explorada por atacantes.
- **Existência de exploits:** existência de ferramentas ou código que podem ser usados para explorar a vulnerabilidade.

4.3. Correção de Vulnerabilidades

A empresa implementará medidas para corrigir as vulnerabilidades identificadas, priorizando as vulnerabilidades mais críticas, de acordo com o seguinte processo:

- **Notificação dos responsáveis:** notificação dos responsáveis pelos sistemas e softwares afetados sobre as vulnerabilidades identificadas.
- **Desenvolvimento de patches:** desenvolvimento de patches ou correções para as vulnerabilidades identificadas.

- **Implementação de medidas de mitigação:** implementação de medidas temporárias para mitigar o risco de exploração das vulnerabilidades enquanto as correções não são implementadas.

4.4. Monitoramento e Revisão

A empresa monitorará continuamente o surgimento de novas vulnerabilidades e revisará periodicamente seu processo de análise de vulnerabilidades 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

- **Vulnerabilidade:** falha de segurança em um sistema de informação e tecnologia que pode ser explorada por um