Política de Análise de Vulnerabilidades para Empresas de Telecomunicações

Baseado no Framework NIST 800-53

2. Propósito

Estabelecer um processo contínuo para identificar, avaliar e remediar vulnerabilidades em sistemas de informação da empresa de telecomunicações, a fim de reduzir o risco de ataques cibernéticos e proteger seus ativos de informação.

3. Escopo

Esta política se aplica a todos os sistemas de informação da empresa, incluindo redes, dispositivos, aplicativos e dados. Abrange todos os colaboradores, independentemente de cargo ou função.

4. Política

A empresa de telecomunicações se compromete a:

- **Realizar análises de vulnerabilidades regulares:** Identificar e avaliar periodicamente as vulnerabilidades existentes em seus sistemas de informação.
- **Priorizar e remediar vulnerabilidades:** Priorizar a correção das vulnerabilidades de acordo com o seu nível de risco e impacto potencial nos negócios.
- **Documentar e reportar:** Documentar os resultados das análises de vulnerabilidades e reportar à alta gerência os riscos e as medidas de remediação tomadas.

5. Procedimentos Relacionados

- **Planejamento:**
  - Definir a frequência das análises de vulnerabilidades.
  - Selecionar ferramentas e métodos adequados para a análise.
  - Identificar os sistemas de informação a serem analisados.
- **Execução:**
  - Realizar a análise de vulnerabilidades de acordo com o plano.
  - Documentar os resultados da análise, incluindo as vulnerabilidades identificadas, seu nível de risco e as medidas de remediação recomendadas.
- **Remediação:**
  - Priorizar a correção das vulnerabilidades de acordo com o seu nível de risco e impacto potencial nos negócios.
  - Implementar medidas de remediação adequadas para cada vulnerabilidade.
  - Monitorar a efetividade das medidas de remediação.
- **Relatório:**
  - Reportar à alta gerência os resultados das análises de vulnerabilidades e as medidas de remediação tomadas.

6. Não Conformidade

O não cumprimento desta política poderá resultar em medidas disciplinares, incluindo advertência verbal, advertência escrita, suspensão ou rescisão de contrato.

7. Compromisso/Autoridade da Gestão

A alta gerência da empresa de telecomunicações se compromete a fornecer os recursos necessários para a implementação e o cumprimento desta política. A equipe de segurança da informação é responsável pela gestão e atualização da política.

8. Cronograma de Revisão

A política será revisada anualmente ou após um incidente de segurança cibernética significativo.

9. Definições

- **Vulnerabilidade:** Fraqueza em um sistema de informação que pode ser explorada por um invasor para obter acesso não autorizado, comprometer a integridade dos dados ou interromper o serviço.
- **Análise de vulnerabilidades:** Processo de identificação, avaliação e priorização de vulnerabilidades em um sistema de informação.
- **Plano de remediação:** Plano que define as medidas a serem tomadas para corrigir as vulnerabilidades identificadas.

Observações:

- Esta política é um exemplo e deve ser adaptada às necessidades específicas da empresa de telecomunicações.
- É importante consultar especialistas em segurança cibernética para a implementação da política.