Política de Resposta a Incidentes de Segurança Cibernética

Baseado no Framework NIST 800-53

2. Propósito

Estabelecer um plano de ação para detectar, conter, mitigar e recuperar-se de incidentes de segurança cibernética, protegendo os ativos de informação da empresa de telecomunicações e minimizando o impacto nos negócios.

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:

- **Detectar:** Monitorar continuamente os sistemas de informação para identificar atividades anormais e potenciais ameaças.
- **Conter:** Limitar o impacto de um incidente de segurança cibernética, isolando os sistemas afetados e restringindo o acesso a dados confidenciais.
- **Mitigar:** Implementar medidas para reduzir a probabilidade e o impacto de futuros incidentes de segurança cibernética.
- **Recuperar:** Restaurar os sistemas de informação e dados afetados a um estado operacional seguro.

5. Procedimentos Relacionados

- **Detecção:**

    - Monitoramento de logs de segurança.
    - Análise de anomalias de rede.
    - Detecção de intrusão.
    - Testes de penetração.
- **Contenção:**
    - Isolamento de sistemas afetados.
    - Desativação de contas de usuários comprometidas.
    - Bloqueio de acesso a dados confidenciais.
- **Mitigação:**
    - Implementação de medidas de segurança técnica e administrativa.
    - Treinamento de colaboradores sobre segurança cibernética.
    - Atualização de software e sistemas.
- **Recuperação:**
    - Restauração de backups de dados.
    - Reconstrução de sistemas afetados.
    - Revisão e aprimoramento dos procedimentos de segurança.

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

- **Incidente de segurança cibernética:** Qualquer evento que possa comprometer a confidencialidade, integridade ou disponibilidade dos sistemas de informação ou dos dados da empresa.
- **Equipe de resposta a incidentes:** Equipe responsável por coordenar a resposta a incidentes de segurança cibernética.
- **Plano de resposta a incidentes:** Documento que descreve os procedimentos a serem seguidos em caso de incidente de segurança cibernética.

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.