Política de Identificação de Riscos em Segurança Cibernética para Empresas de Energia e Utilidades

Baseado no Framework CSF 2.0

2. Propósito

Estabelecer um processo formal para identificar, avaliar e priorizar os riscos de segurança cibernética que podem afetar os ativos de informação da empresa de energia e utilidades, a fim de proteger a confidencialidade, integridade e disponibilidade dos dados críticos da infraestrutura.

3. Escopo

Esta política se aplica a todos os ativos de informação da empresa, incluindo:

- **Sistemas de informação:** Computadores, servidores, redes, dispositivos móveis, softwares e aplicações.
- **Dados:** Informações sobre clientes, fornecedores, operações, finanças, projetos e outros dados confidenciais.
- **Equipamentos de controle industrial:** Sistemas de controle e monitoramento de infraestrutura crítica, como usinas de energia, redes de distribuição e sistemas de gás.

4. Política

A empresa de energia e utilidades se compromete a:

- **Identificar todos os riscos de segurança cibernética:** Realizar avaliações de risco regulares para identificar os riscos potenciais que podem afetar os ativos de informação da empresa.
- **Avaliar os riscos de segurança cibernética:** Analisar os riscos identificados para determinar sua probabilidade de ocorrência e impacto potencial nos negócios.
- **Priorizar os riscos de segurança cibernética:** Classificar os riscos de acordo com sua severidade e tomar medidas para mitigar os riscos mais críticos.
- **Monitorar os riscos de segurança cibernética:** Monitorar continuamente o ambiente de segurança cibernética para identificar novos riscos e avaliar a efetividade das medidas de mitigação.

5. Procedimentos Relacionados

- **Avaliação de riscos:**
  - Realizar avaliações de risco regulares utilizando metodologias como o NIST Cybersecurity Framework (CSF) e o ISO/IEC 27001.
  - Envolver stakeholders relevantes no processo de avaliação de riscos.
- **Análise de riscos:**
  - Analisar os riscos identificados para determinar sua probabilidade de ocorrência e impacto potencial nos negócios.
  - Quantificar o impacto potencial dos riscos em termos financeiros, operacionais e reputacionais.
- **Priorização de riscos:**
  - Classificar os riscos de acordo com sua severidade e tomar medidas para mitigar os riscos mais críticos.
  - Definir critérios claros para a priorização dos riscos.

- **Monitoramento de riscos:**
  - Monitorar continuamente o ambiente de segurança cibernética para identificar novos riscos e avaliar a efetividade das medidas de mitigação.
  - Implementar um sistema de alerta para notificar os stakeholders sobre novos riscos ou mudanças no perfil de risco.

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 energia e utilidades 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

- **Risco de segurança cibernética:** Probabilidade de um evento que possa causar perda, confidencialidade, integridade ou disponibilidade dos ativos de informação.
- **Avaliação de riscos:** Processo de identificação, análise e avaliação dos riscos de segurança cibernética.
- **Análise de riscos:** Processo de determinar a probabilidade de ocorrência de um risco e o impacto potencial que ele pode ter nos negócios.

- **Priorização de riscos:** Processo de classificação dos riscos de acordo com sua severidade.
- **Monitoramento de riscos:** Processo de acompanhar e avaliar os riscos de segurança cibernética ao longo do tempo.

Observações:

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