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

Baseado no Framework CSF 2.0

2. Propósito

Estabelecer um processo formal para identificar, classificar e controlar 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 ativos de informação:** Criar e manter um inventário completo de todos os ativos de informação, incluindo sua localização, função e nível de criticidade.

- **Classificar os ativos de informação:** Categorizar os ativos de acordo com o seu valor, confidencialidade e impacto potencial em caso de perda ou violação.
- **Controlar o acesso aos ativos de informação:** Implementar medidas de segurança para controlar o acesso aos ativos de informação, incluindo autenticação, autorização e criptografia.
- **Proteger os ativos de informação contra perda, roubo ou danos:** Implementar medidas de segurança para proteger os ativos de informação contra perda, roubo ou danos, como backups, recuperação de desastres e controles de acesso físico.

5. Procedimentos Relacionados

- **Inventário de ativos:**
  - Realizar um inventário completo de todos os ativos de informação, incluindo sua localização, função e nível de criticidade.
  - Atualizar o inventário regularmente para refletir as mudanças nos ativos de informação.
- **Classificação de ativos:**
  - Criar um sistema de classificação para categorizar os ativos de acordo com o seu valor, confidencialidade e impacto potencial em caso de perda ou violação.
  - Aplicar a classificação de ativos a todos os novos ativos de informação.
- **Controle de acesso:**
  - Implementar medidas de segurança para controlar o acesso aos ativos de informação, incluindo autenticação, autorização e criptografia.
  - Revisar e atualizar os controles de acesso regularmente.
- **Proteção de ativos:**

- Implementar medidas de segurança para proteger os ativos de informação contra perda, roubo ou danos, como backups, recuperação de desastres e controles de acesso físico.
- Monitorar a efetividade das medidas de proteção de ativos.

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

- **Ativo de informação:** Qualquer informação ou dado que tenha valor para a empresa.
- **Confidencialidade:** A garantia de que apenas as pessoas autorizadas podem acessar os dados.
- **Integridade:** A garantia de que os dados são precisos e completos.
- **Disponibilidade:** A garantia de que os dados estão acessíveis quando necessário.

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.