Política de Controle de Acesso para Segurança Cibernética em Empresas Financeiras

Baseada no Framework NIST 800-53

2. Propósito

Estabelecer regras e procedimentos para o controle de acesso aos recursos de informação e tecnologia da empresa, visando garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas.

3. Escopo

Aplica-se a todos os usuários dos recursos de informação e tecnologia da empresa, incluindo:

- **Funcionários:** colaboradores, terceirizados, prestadores de serviço, etc.
- **Clientes:** pessoas físicas e jurídicas que utilizam os serviços da empresa.
- **Parceiros:** empresas e instituições que possuem relacionamento comercial com a empresa.

4. Política

4.1. Níveis de Acesso

O acesso aos recursos de informação e tecnologia da empresa será concedido de acordo com a necessidade de cada usuário, com base nos seguintes níveis de acesso:

- **Administrador:** acesso total a todos os recursos.

- **Usuário:** acesso a recursos específicos de acordo com a função do usuário.
- **Visitante:** acesso limitado a recursos específicos.

4.2. Autenticação e Autorização

O acesso aos recursos de informação e tecnologia da empresa será controlado por meio de mecanismos de autenticação e autorização, como:

- **Login e senha:** combinação de nome de usuário e senha para autenticação.
- **Cartões de acesso:** cartões inteligentes ou biométricos para autenticação.
- **Tokens de segurança:** dispositivos físicos para autenticação.
- **Permissões de acesso:** regras que definem quais recursos cada usuário pode acessar.

4.3. Gerenciamento de Acessos

A empresa manterá um processo formal para gerenciar os acessos aos recursos de informação e tecnologia, incluindo:

- **Concessão de acessos:** análise e aprovação de solicitações de acesso.
- **Revisão de acessos:** revisão periódica dos acessos concedidos para garantir que ainda sejam necessários.
- **Revogação de acessos:** revogação de acessos quando não forem mais necessários.

5. Procedimentos Relacionados

- Política de Segurança da Informação
- Política de Senhas
- Política de Controle de Mudanças

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 e com a proteção dos dados. A equipe de TI é responsável pela implementação e monitoramento desta política.

8. Cronograma de Revisão

Esta política será revisada anualmente ou quando necessário.

9. Definições

- **Controle de acesso:** conjunto de medidas que visam controlar quem pode acessar quais recursos de informação e tecnologia.
- **Autenticação:** processo de verificar a identidade de um usuário.
- **Autorização:** processo de determinar quais recursos um usuário pode acessar.
- **Permissões de acesso:** regras que definem quais recursos cada usuário pode acessar.

Observações:

- Esta política é um exemplo e pode ser adaptada às necessidades específicas da empresa.

- É importante consultar especialistas em segurança da informação para auxiliar na implementação da política.