Política de Autenticação para Segurança Cibernética em Empresas Financeiras

Baseada no Framework NIST 800-53

2. Propósito

Estabelecer regras e procedimentos para a autenticação de usuários nos 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. Fatores de Autenticação

A autenticação dos usuários nos recursos de informação e tecnologia da empresa será realizada por meio de, no mínimo, dois fatores de autenticação, como:

- **Fator de posse:** algo que o usuário possui, como um cartão de acesso ou token de segurança.
- **Fator de conhecimento:** algo que o usuário sabe, como uma senha ou PIN.
- **Fator de inerência:** algo que o usuário é, como uma característica biométrica.

4.2. Métodos de Autenticação

A empresa utilizará os seguintes métodos de autenticação:

- **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.
- **Autenticação biométrica:** reconhecimento de digital, íris ou facial para autenticação.

4.3. Gerenciamento de Credenciais

A empresa manterá um processo formal para gerenciar as credenciais de acesso dos usuários, incluindo:

- **Criação de credenciais:** definição de regras para a criação de senhas e PINs fortes.
- **Armazenamento de credenciais:** armazenamento seguro das credenciais de acesso.
- **Alteração de credenciais:** periodicidade para alteração de senhas e PINs.
- **Revogação de credenciais:** revogação de credenciais quando não forem mais necessárias.

5. Procedimentos Relacionados

- Política de Segurança da Informação

- Política de Controle de Acesso
- Política de Senhas

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

- **Autenticação:** processo de verificar a identidade de um usuário.
- **Fator de autenticação:** característica que ajuda a verificar a identidade de um usuário.
- **Credencial de acesso:** informação utilizada para autenticar um usuário em um sistema de informação.

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.