Política de Senhas e Autenticação

1. Objetivo:

1.1 Esta política estabelece as diretrizes para a criação, uso e proteção de senhas, bem como os requisitos de autenticação para o acesso a sistemas da organização.

2. Senhas:

2.1 As senhas são um componente essencial da segurança da informação. Para garantir a proteção adequada, as seguintes diretrizes devem ser seguidas:

- As senhas devem ter no mínimo oito caracteres.
- Devem incluir uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.
- As senhas não devem ser facilmente relacionadas a informações pessoais (como nomes, datas de nascimento, etc.).
- As senhas devem ser alteradas regularmente, a cada 6 (seis) meses.
- Senhas não devem ser compartilhadas ou divulgadas a terceiros.

3. Autenticação de Dois Fatores (2FA):

3.1 A autenticação de dois fatores (2FA) é uma camada adicional de segurança. De acordo com esta política:

- A 2FA deve ser habilitada para todos os sistemas e aplicativos que oferecem suporte a essa funcionalidade.
- O uso da 2FA é obrigatório para o acesso a sistemas e informações críticas.

4. Proteção de Senhas:

4.1 Para garantir a segurança das senhas armazenadas e transmitidas, as seguintes medidas devem ser tomadas:

- Senhas não devem ser armazenadas em formatos legíveis. Em vez disso, devem ser adequadamente criptografadas.
- A transmissão de senhas deve ocorrer por meio de canais seguros, com protocolos de criptografia.

5. Gerenciamento de Acesso:

5.1 O acesso a sistemas e informações deve ser gerenciado de acordo com o princípio do menor privilégio:

5.1.1 Cada usuário deve receber acesso apenas às informações e recursos necessários para desempenhar suas funções.

5.1.2 O acesso deve ser revisto regularmente e ajustado conforme necessário.

6. Monitoramento e Auditoria:

6.1 A organização reserva-se o direito de monitorar o uso de senhas e conduzir auditorias de segurança para garantir a conformidade com esta política.

6.2 Tentativas suspeitas de acesso ou violações de senha devem ser relatadas imediatamente à equipe de segurança da informação.

7. Conscientização e Treinamento:

7.1 A organização fornecerá treinamentos regulares sobre boas práticas de segurança da informação, incluindo a criação e gestão de senhas seguras.

8. Disposições Finais:

8.1 O não cumprimento desta política pode resultar em medidas disciplinares, incluindo rescisão de contrato e responsabilização por eventuais danos causados.

8.2 Alterações nesta política serão comunicadas aos usuários de forma eficaz.