Políticas de Segurança da Informação

Proposta para a Empresa AlfaTech Soluções Criativas

Desenvolvido por:
Felipe Pereira do Nascimento - RA 825126069
Guilherme Dourado Nascimento – RA: 825116419
Bruno de Oliveira Santos – RA: 823223513
Pedro Miranda Rabelo – RA: 825243591
Kauane Sandes Brandão - RA: 825113309
Stephany Ramos Rodrigues - RA 82512339

Data: Outubro de 2025

Versão: 1.0

Sumário

1. **Introdução**
2. **Política de Acesso e Controle de Usuários**
    a. 2.1. Criação e Desativação de Contas
    b. 2.2. Princípio do Menor Privilégio
    c. 2.3. Política de Senhas Fortes
    d. 2.4. Bloqueio de Estações de Trabalho
    e. 2.5. Justificativas
3. **Política de Uso de Dispositivos Móveis e Redes (BYOD)**
    a. 3.1. Uso de Dispositivos Pessoais (BYOD)
    b. 3.2. Segurança da Rede Wi-Fi
    c. 3.3. Justificativas
4. **Diretrizes para Resposta a Incidentes de Segurança**
    a. 4.1. Identificação e Notificação
    b. 4.2. Plano de Ação (Fases)
    c. 4.3. Justificativas
5. **Política de Backup e Recuperação de Desastres**

a. 5.1. Estratégia de Backup 3-2-1
b. 5.2. Frequência e Retenção
c. 5.3. Testes de Recuperação
d. 5.4. Justificativas
6. **Termo de Responsabilidade e Aceite**

1. Introdução

Este documento estabelece as Políticas de Segurança da Informação para a "AlfaTech Soluções Criativas". O objetivo é proteger os ativos de informação da empresa e de seus clientes contra ameaças, garantir a continuidade dos negócios, minimizar riscos e assegurar a conformidade com leis e regulamentos, como a Lei Geral de Proteção de Dados (LGPD). A segurança é uma responsabilidade de todos os colaboradores.

2. Política de Acesso e Controle de Usuários

Objetivo: Garantir que apenas pessoas autorizadas tenham acesso aos sistemas e dados, seguindo o princípio do menor privilégio.

2.1. Criação e Desativação de Contas:

- **Admissão:** Novas contas de usuário devem ser solicitadas pelo setor Administrativo/RH e criadas pelo responsável de TI com o nível mínimo de acesso.
- **Desligamento:** A conta de um colaborador desligado deve ser imediatamente desativada no seu último dia de trabalho.

2.2. Princípio do Menor Privilégio:

- Usuários terão permissão de acesso somente aos dados e sistemas essenciais para suas funções. Revisões de acesso serão realizadas semestralmente.

2.3. Política de Senhas Fortes:

- As senhas devem ter no mínimo 12 caracteres, com letras maiúsculas, minúsculas, números e símbolos.
- A troca de senha será obrigatória a cada 90 dias.
- É obrigatório o uso de **Autenticação de Múltiplos Fatores (MFA)** em todos os serviços críticos.

2.4. Bloqueio de Estações de Trabalho:

- É obrigatório o bloqueio da tela do computador sempre que o colaborador se ausentar de sua mesa.

2.5. Justificativas: O controle rigoroso de contas e o princípio do menor privilégio limitam a exposição em caso de comprometimento. Senhas fortes e MFA são a barreira mais eficaz contra o roubo de credenciais, enquanto o bloqueio de tela protege contra acesso físico não autorizado.

3. Política de Uso de Dispositivos Móveis e Redes (BYOD)

Objetivo: Proteger as informações da empresa acessadas em dispositivos móveis e garantir a segurança da rede corporativa.

3.1. Uso de Dispositivos Pessoais (BYOD):

- Para acessar dados corporativos, o dispositivo pessoal deve possuir senha, PIN ou biometria para desbloqueio de tela.
- Em caso de perda ou roubo, o colaborador deve comunicar o responsável de TI imediatamente para revogação dos acessos.

3.2. Segurança da Rede Wi-Fi:

- Haverá duas redes: **`AlfaTech_Corp`** (segura, para colaboradores) e **`AlfaTech_Visitantes`** (isolada, para visitantes).

- É proibido conectar dispositivos da empresa a redes Wi-Fi públicas sem o uso de uma **VPN (Virtual Private Network)**.

3.3. Justificativas: Dispositivos móveis são vulneráveis a perda e roubo, exigindo segurança mínima. A segmentação da rede Wi-Fi impede que ameaças na rede de visitantes afetem a rede corporativa. O uso de VPN em redes públicas criptografa a comunicação, prevenindo a interceptação de dados.

4. Diretrizes para Resposta a Incidentes de Segurança

Objetivo: Estabelecer um plano de ação claro para identificar, conter, erradicar e se recuperar de um incidente de segurança.

4.1. Identificação e Notificação:

- Qualquer suspeita de incidente de segurança deve ser **imediatamente** notificada ao responsável de TI.
- Não tente resolver o problema sozinho. Desconecte o equipamento da rede e aguarde instruções.

4.2. Plano de Ação (Fases):

1. **Contenção:** Isolar o sistema afetado da rede.
2. **Análise:** Investigar a causa e a extensão do incidente.
3. **Erradicação:** Remover a ameaça do ambiente.
4. **Recuperação:** Restaurar os sistemas a partir de backups seguros.
5. **Pós-Incidente:** Documentar o ocorrido e implementar melhorias.

4.3. Justificativas: Um plano de resposta transforma o pânico em uma ação organizada, minimizando os danos. A notificação rápida e a preservação de evidências são cruciais para entender a falha e evitar reincidências.

5. Política de Backup e Recuperação de Desastres

Objetivo: Garantir que os dados críticos da empresa possam ser recuperados de forma rápida e confiável.

5.1. Estratégia de Backup 3-2-1:

- Manter **3 cópias** dos dados, em **2 mídias diferentes**, com **1 cópia fora do local** (offsite, na nuvem).

5.2. Frequência e Retenção:

- Backups diários (retidos por 30 dias) e mensais (retidos por 1 ano).

5.3. Testes de Recuperação:

- Testes de restauração devem ser realizados trimestralmente para garantir a integridade dos backups.

5.4. Justificativas: A estratégia 3-2-1 oferece alta resiliência contra falhas e desastres. Backups testados são a principal defesa contra ataques de ransomware, permitindo a recuperação dos dados sem a necessidade de pagar resgate e assegurando a continuidade dos negócios.

6. Termo de Responsabilidade e Aceite

Eu, [Nome do Colaborador], declaro que li, compreendi e concordo em cumprir todas as Políticas de Segurança da Informação estabelecidas neste documento pela AlfaTech Soluções Criativas.

Entendo que o não cumprimento destas políticas pode resultar em medidas disciplinares, conforme as normas internas da empresa e a legislação vigente.

Assinatura do Colaborador

Data: ____ / ____ / ____