**UNIVERSIDADE SÃO JUDAS TADEU**

**Sistemas Computacionais e Segurança**

*Isabelle de Godoy Sanchez*

*Kathleen Lohanny de Souza*

*Kauã Santana Oliveira*

*Pedro Henrique Ferreira da Rocha*

*Pedro Henrique Ribeiro Baptista*

*Richard Rosa Galindo*

**Políticas de Segurança da Informação**

A segurança da informação é fundamental para proteger os ativos digitais e garantir a continuidade dos negócios. Este documento apresenta um conjunto de políticas básicas desenvolvidas para uma pequena empresa fictícia chamada TechSafe Soluções Digitais, com o objetivo de estabelecer boas práticas, prevenir incidentes e mitigar riscos.

As políticas a seguir foram elaboradas com base em princípios de confidencialidade, integridade e disponibilidade da informação.

**1. Política de Acesso e Controle de Usuários**

Todos os usuários devem possuir credenciais únicas para acesso aos sistemas corporativos. É obrigatório o uso de senhas fortes, autenticação multifator e revisão periódica de permissões.

**Diretrizes principais:**

* Criação de contas somente mediante solicitação formal e aprovação do gestor.
* Senhas devem conter letras maiúsculas, minúsculas, números e caracteres especiais.
* Contas inativas por mais de 30 dias serão bloqueadas.
* Autenticação de dois fatores obrigatória para acesso remoto.

Justificativa:

O controle individualizado impede acessos indevidos e facilita auditorias, reduzindo riscos de vazamento de dados.

**2. Política de Uso de Dispositivos Móveis e Redes**

Dispositivos móveis corporativos devem seguir padrões de segurança e não podem ser utilizados para fins pessoais. O acesso a redes sem fio deve ser feito apenas em conexões seguras.

**Diretrizes principais:**

* É proibido conectar dispositivos pessoais a sistemas corporativos.
* Uso obrigatório de VPN ao acessar informações fora da empresa.
* Wi-Fi corporativo deve possuir senha forte e criptografia WPA3.
* Instalação de antivírus e bloqueio remoto em todos os dispositivos móveis.

Justificativa:

Protege dados contra interceptação, roubo de credenciais e infecção por malware, especialmente em ambientes externos.

**3. Diretrizes para Resposta a Incidentes de Segurança**

Define o processo de identificação, comunicação, contenção e resolução de incidentes de segurança da informação.

**Diretrizes principais:**

* Todos os colaboradores devem reportar incidentes imediatamente ao setor de TI.
* O time de resposta deve conter profissionais treinados para isolar sistemas comprometidos.
* Devem ser mantidos registros (logs) detalhados de cada incidente.
* Após a contenção, realizar análise de causa e plano de prevenção.

Justificativa:

Permite uma resposta rápida e eficiente, minimizando danos e aprendendo com os eventos para evitar recorrência.

**4. Política de Backup e Recuperação de Desastres**

Garante a continuidade operacional por meio de cópias seguras e planos de restauração de dados.

**Diretrizes principais:**

* Backup diário automático em servidores locais e na nuvem.
* Testes mensais de restauração.
* Armazenamento de cópias em locais distintos.
* Criação de um plano de continuidade de negócios (BCP).

Justificativa:

Essencial para recuperar informações em caso de falhas, ataques cibernéticos ou desastres naturais.

**Conclusão**

A implementação dessas políticas estabelece uma base sólida de segurança, reforçando a cultura de proteção da informação e garantindo maior confiabilidade às operações da TechSafe Soluções Digitais.