Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

ATIVIDADADE 1

POLÍTICAS DE SEGURANÇA DE UMA EMPRESA

João Vitor Chioatto Serafim – 825133189

João Victor de Souza - 825135230

Professor: Robson Calvetti

São Paulo – SP

2025

JJ TECH

Segue abaixo manual de **políticas de segurança da empresa JJ TECH.**

1. Política de Acesso e Controle de Usuários

Define regras para criação, uso e controle das contas de usuários e sistemas internos da empresa.

Regras principais:

- Cada colaborador deve possuir usuário e senha individual;
- Senhas devem ser trocadas a cada 90 dias;
- É proibido o compartilhamento de senhas;
- Contas de ex-funcionários devem ser imediatamente desativadas;
- Implementar autenticação em dois fatores (2FA) sempre que possível.

Justificativa: O controle individual de acessos impede usos indevidos, facilita auditorias e reduz o risco de vazamento de informações internas.

2. Política de Uso de Dispositivos Móveis e Redes

Estabelece normas para o uso de celulares, notebooks e conexões de rede dentro e fora da empresa.

Regras principais:

- Apenas dispositivos autorizados e registrados podem acessar o Wi-Fi interno;
- É proibido conectar pendrives, HDs externos ou dispositivos pessoais sem permissão;
- Dados da empresa em dispositivos móveis devem ser protegidos com senha e bloqueio automático;
- O acesso remoto aos sistemas só pode ser feito via VPN (conexão segura).

Justificativa: Evita contaminação por vírus, acesso indevido e vazamento de informações por meio de dispositivos não monitorados.

3. Diretrizes para Resposta a Incidentes de Segurança

Define os procedimentos que devem ser seguidos em caso de falhas, ataques, perda ou vazamento de dados.

Etapas principais:

- Identificar e registrar o incidente imediatamente;
- Isolar o sistema afetado para impedir a propagação;
- Comunicar o responsável de TI e a direção;
- Investigar a causa e aplicar correções;
- Registrar lições aprendidas e ações preventivas futuras.

Justificativa: Ter um plano de resposta evita improvisos e garante agilidade, minimizando danos financeiros e à reputação da empresa.

4. Política de Backup e Recuperação de Desastres

Define como os dados e sistemas da empresa serão copiados e recuperados em caso de falhas, exclusão acidental ou incidentes.

Regras principais:

- Realizar backup diário automático de arquivos e bancos de dados;
- Manter cópias de segurança em nuvem e em armazenamento físico externo;
- Testar a restauração de backups mensalmente;
- Manter os backups armazenados por pelo menos 6 meses.

Justificativa: Garante a continuidade dos negócios, evitando perda de informações críticas e longos períodos de inatividade.