Políticas de Segurança da Informação

1. Política de Acesso e Controle de Usuários

Todos os usuários devem possuir contas individuais e intransferíveis. O acesso será concedido com base no princípio do menor privilégio.

- Autenticação com senha forte e autenticação em dois fatores (2FA).

  Exemplo:

  Um colaborador acessa o sistema interno da empresa usando:

  Usuário: joao.silva

  Senha: `Jo@0SilvA2025!`

  O sistema exige que a senha:

  Tenha no mínimo 12 caracteres

  Misture letras maiúsculas, minúsculas, números e símbolos

  Seja trocada a cada 90 dias

- Contas inativas por mais de 30 dias serão desativadas automaticamente.
- Acesso administrativo apenas para usuários autorizados.

Reduz riscos de acesso não autorizado e garante rastreabilidade em caso de incidentes.

2. Política de Uso de Dispositivos Móveis e Redes

É permitido o uso de dispositivos pessoais (BYOD), desde que sigam os requisitos mínimos de segurança.

- Dispositivos devem estar atualizados e protegidos com senha.
- É obrigatório o uso de VPN para acesso remoto à rede interna.
- Em caso de perda ou roubo, o setor de TI deve ser notificado imediatamente.

3. Diretrizes para Resposta a Incidentes de Segurança

Definir um processo estruturado e eficiente para detectar, registrar, conter, comunicar e resolver incidentes de segurança, minimizando danos e evitando recorrência.

- Todos os funcionários devem estar treinados para identificar e relatar comportamentos suspeitos ou incidentes (como phishing, acesso não autorizado, falhas de sistema ou vazamento de dados).
- Um canal oficial e seguro (como e-mail específico ou sistema de chamados) deve ser utilizado para a comunicação de incidentes.
- A equipe de segurança deve agir imediatamente para conter o incidente e proteger os ativos da empresa.
- Um relatório detalhado do incidente deve ser elaborado, incluindo: causa raiz, impacto, medidas adotadas e plano de prevenção.
- Sempre que possível, deve-se realizar uma simulação de incidentes periodicamente para testar a eficiência do plano de resposta.

Ter uma resposta rápida e bem definida reduz o tempo de exposição a ameaças, diminui impactos operacionais e protege a imagem da empresa perante seus clientes e parceiros.

4. Política de Backup e Recuperação de Desastres

Todos os dados críticos devem ser incluídos em rotinas de backup e testes periódicos de restauração.

- Backups diários automatizados e criptografados.

    Evita perda de dados recentes;

    Garante que qualquer modificação feita no dia não seja perdida;

É ideal para empresas que lidam com dados constantemente

- Armazenamento em local seguro (nuvem e físico).

  Exemplo: AWS e Microsoft Azure.

- Testes de recuperação devem ser feitos trimestralmente.

Garante a continuidade do negócio em caso de falhas, ataques ou desastres naturais.