# Políticas de Segurança da Informação

Empresa: Look Investimentos

Nosso grupo desenvolveu este conjunto de políticas pensando na segurança das informações da empresa Look Investimentos, que trabalha com soluções financeiras e atende clientes de diferentes regiões do Brasil. Como a empresa conta com 400 funcionários e utiliza diversas ferramentas digitais, achamos importante definir regras para proteger os dados e os sistemas usados no dia a dia.

## 1. Política de Acesso e Controle de Usuários

O que propomos:  
Cada funcionário deve ter um login individual com senha forte e autenticação em duas etapas para acessar os sistemas da empresa, como Microsoft 365, Teams e Trello. Os acessos devem ser definidos conforme o cargo de cada um, para evitar que pessoas tenham acesso a informações desnecessárias.

Justificativa:  
Com isso, conseguimos controlar melhor quem acessa o quê, o que ajuda a evitar vazamentos de dados e erros causados por acessos indevidos.

## 2. Uso de Dispositivos e Conexões

O que propomos:  
Os dispositivos usados pelos funcionários (notebooks, celulares, etc.) devem ter antivírus atualizado e proteção com senha. O uso de redes Wi-Fi públicas deve ser evitado, e o acesso remoto aos sistemas da empresa precisa ser feito por VPN. Dispositivos pessoais só devem ser usados com autorização da equipe de TI.

Justificativa:  
Essas medidas ajudam a manter a segurança das informações mesmo quando os funcionários estão fora da empresa, já que muitas das ferramentas utilizadas são online e baseadas em nuvem.

## 3. Respostas a Incidentes de Segurança

O que propomos:  
Caso ocorra algum problema como ataque de vírus, tentativa de invasão ou qualquer situação suspeita, o funcionário deve comunicar imediatamente a equipe de TI. A empresa deve seguir um plano com etapas para resolver o problema, entender o que causou e registrar tudo para futuras prevenções.

Justificativa:  
Ter um processo claro evita confusão e ajuda a resolver problemas mais rapidamente, reduzindo os impactos no funcionamento da empresa.

## 4. Backup e Recuperação de Dados

O que propomos:  
Os dados importantes da empresa devem ser salvos diariamente, tanto na nuvem quanto em servidores locais. Também é importante fazer testes regulares para garantir que os backups estejam funcionando corretamente.

Justificativa:  
Esses cuidados garantem que a empresa não perca informações importantes em caso de falhas técnicas, ataques ou até erros humanos.