Políticas de Segurança da Informação

Empresa: \*\*SecureTech Solutions LTDA\*\*

Alunos: Rodolfo Regis de Souza – RA 825113514

Sergio Rycbzak Junior – RA 825154823

Pietro Oliveira Silva – RA 825113483

Gabriel Souza Santos – RA 825113168

Professor: Calvetti

Instituição: Universidade São Judas Tadeu – Campus Mooca

Curso: Análise e Desenvolvimento de Sistemas

# ATIVIDADE 1 — Desenvolvimento de Políticas de Segurança para uma Pequena Empresa

## 1. Identificação da Empresa Fictícia

Nome: SecureTech Solutions LTDA

Ramo de atuação: Desenvolvimento de software e suporte técnico para pequenas empresas.

Número de funcionários: 15

Infraestrutura: Rede interna com servidor local, notebooks corporativos e acesso remoto via VPN.

## 2. Política de Acesso e Controle de Usuários

Objetivo: Garantir que apenas pessoas autorizadas acessem informações e sistemas internos.  
  
Diretrizes:  
- Cada colaborador deve possuir usuário e senha individuais.  
- Senhas devem ter mínimo de 8 caracteres, com letras, números e símbolos.  
- Troca de senha obrigatória a cada 90 dias.  
- Contas inativas por mais de 30 dias devem ser desativadas.  
- Acesso administrativo concedido apenas a pessoal de TI autorizado.  
  
Justificativa: Reduz o risco de acesso indevido, vazamento de informações e uso não autorizado de sistemas internos.

## 3. Política de Uso de Dispositivos Móveis e Redes

Objetivo: Proteger os dados corporativos em dispositivos móveis e conexões externas.  
  
Diretrizes:  
- É proibido conectar pendrives pessoais ou dispositivos sem autorização.  
- Dispositivos móveis corporativos devem ter senha de bloqueio e criptografia habilitada.  
- Conexões fora da empresa devem usar VPN.  
- Wi-Fi corporativo deve ter senha forte e ser alterada periodicamente.  
  
Justificativa: Evita vazamentos de dados e invasões via conexões inseguras ou dispositivos contaminados.

## 4. Diretrizes para Resposta a Incidentes de Segurança

Objetivo: Garantir reação rápida e organizada em caso de falha ou ataque.  
  
Procedimentos:  
1. Identificação: Relatar imediatamente incidentes à equipe de TI.  
2. Contenção: Isolar o sistema afetado.  
3. Erradicação: Remover a causa (malware, acesso indevido, etc.).  
4. Recuperação: Restaurar o sistema a partir do backup.  
5. Análise Pós-incidente: Documentar o ocorrido e aplicar melhorias preventivas.  
  
Justificativa: Minimiza o impacto de falhas e melhora a segurança contínua da empresa.

## 5. Política de Backup e Recuperação de Desastres

Objetivo: Garantir que os dados críticos possam ser recuperados após falhas ou ataques.  
  
Diretrizes:  
- Realizar backup diário automático em servidor seguro.  
- Cópia semanal armazenada na nuvem.  
- Testar a restauração dos backups mensalmente.  
- Manter registro dos backups realizados.  
  
Justificativa: Evita perda de informações importantes em caso de ataques de ransomware, falhas de hardware ou desastres.

## 6. Conclusão

Essas políticas formam a base da segurança da informação da SecureTech Solutions LTDA, promovendo integridade, confidencialidade e disponibilidade dos dados.