Desenvolvimento de Políticas de Segurança para uma Pequena Empresa

Participantes:
Otavio Paiva Silva:824147017
Gabriel Prieto Lima: 824142064
Eduardo Baptistella: 824147595

Políticas de Acesso dos Usuários:

Estabeleça diretrizes claras sobre o acesso a sistemas e informações para garantir que apenas usuários autorizados tenham acesso a dados confidenciais.

Diretrizes:

Todos os usuários devem utilizar uma senha forte (pelo menos 9 caracteres, incluindo letras maiusculas, minúsculas, números e caracteres especiais) e alterar suas senhas a cada 90 dias.
Níveis de acesso: O acesso aos dados e sistemas será baseado na função do usuário (princípio do menor privilégio). Cada colaborador tem acesso apenas às informações necessárias ao desempenho de suas funções.
Registro de acesso: Todos os acessos a sistemas críticos serão registrados e auditados mensalmente para detectar possíveis anomalias.

Justificativa para prevenir acessos não autorizados:

Essas diretrizes ajudam a prevenir acessos não autorizados, minimizar o risco de divulgação de informações e garantir que cada colaborador tenha acesso apenas ao necessário para suas atividades.

Políticas para uso dos dispositivos Móveis e Redes:

Regular o uso de dispositivos móveis e o acesso à rede para proteger as informações da empresa.
Guia do Uso de Dispositivos Móveis: Dispositivos pessoais podem ser utilizados para acessar informações da empresa, desde que protegidos por senha e tenham software de segurança instalado.
Conecte-se à rede: Acesse a rede corporativa somente através de uma rede Wi-Fi segura. Redes públicas devem ser evitadas ou feitas usando VPN.

Relatar perda ou roubo: Se um dispositivo for perdido ou roubado, os usuários deverão reportar imediatamente à equipe de TI para que medidas de segurança possam ser implementadas.

Justificativa: Essas diretrizes visam proteger os dados da empresa contra acessos não autorizados e vazamentos, especialmente em ambientes menos seguros.

Diretrizes para Resposta a Incidentes de Segurança
Objetivo:

Guia de resposta a incidentes de segurança
objetivo
Processos bem definidos para identificar, responder e recuperar-se de incidentes de segurança.
Guia De Reconhecimento de Incidentes: Todos os funcionários devem ser treinados para identificar e relatar incidentes de segurança.
Equipe de Resposta: Monte uma equipe de resposta a incidentes (ERI) composta por membros da equipe de TI e de gerenciamento.
Plano de Resposta: As ERI devem seguir um plano escrito para responder a um incidente, incluindo contenção, erradicação, recuperação e comunicação com as partes interessadas.
razão

Justificativa:

A resposta eficaz a incidentes é fundamental para minimizar perdas e proteger os ativos de informação. A formação e a preparação garantem uma ação rápida e coordenada.

Política de Backup e Recuperação dos dado

Garantir que o backup dos dados da empresa seja feito regularmente e que possam ser recuperados em caso de perda de dados ou desastre.

Diretrizes

Frequência de backup: O backup dos dados críticos deve ser feito diariamente, enquanto o backup dos dados menos confidenciais pode ser feito semanalmente.

Armazenamento: os backups devem ser armazenados em local seguro, preferencialmente fora do local físico da empresa, para proteção contra desastres locais.

Testes de recuperação: os testes de recuperação de dados devem ser realizados a cada seis meses para garantir que os backups funcionem e possam ser restaurados.
Justificação
É essencial garantir a continuidade das atividades e a proteção dos dados. Backups regulares e testes de recuperação minimizam o impacto da perda de dados.

Conclusões:

As políticas apresentadas são essenciais para criar uma base sólida para a segurança da informação em Tech Solutions. Implementar e seguir estas diretrizes ajudará a proteger os ativos da empresa e a criar um ambiente de trabalho seguro. É fundamental que todos os colaboradores sejam treinados e estejam cientes dessas políticas para garantir sua eficácia.