Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

Prof. Robson Calvetti

João Luiz Da Silva e Rafael Tiago Scisci Arciénega

RA: 82420546 e 824216105

Pesquisa: Desenvolvimento de Políticas de Segurança para uma Pequena Empresa

Objetivo: Criar um conjunto de básico de políticas de segurança da informação para nossa empresa, composto por:

-Políticas de acesso e controle de usuários:

* Autenticação Forte: Nossos funcionários devem usar suas próprias senhas, que devem possuir: no mínimo, 8 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos.

*Privilégios de acesso: O acesso a informações e sistemas deve ser limitado apenas as atividades necessárias dos funcionários.

*Revisão de acessos: Devem ser revisadas trimestralmente para garantir que as permissões estejam atualizadas e que ex-colaboradores tenham seus acessos anulados.

*MFA: Sempre deve ser executada para melhorar a segurança de contas com acesso crítico.

- Política de uso de dispositivos móveis e redes;

Uso de Dispositivos: Dispositivos móveis utilizados para acessar dados da empresa devem estar protegidos com senha ou biometria e ter soluções de segurança, como antivírus e criptografia, instaladas.

Conexões Seguras: O uso de redes Wi-Fi públicas para acessar dados da empresa é estritamente proibido, a menos que uma VPN segura esteja em uso.

Aplicativos Permitidos: Apenas aplicativos e softwares aprovados pela equipe de TI podem ser instalados em dispositivos que acessam informações corporativas.

Reportar Perda/Roubo: Qualquer dispositivo móvel perdido ou roubado deve ser reportado à equipe de TI imediatamente para que possam ser tomadas as ações necessárias.

- Diretrizes para resposta a incidentes de segurança;

Identificação de Incidentes: Todos os colaboradores devem ser treinados para reconhecer sinais de incidentes de segurança, como e-mails suspeitos ou acessos não autorizados.

Notificação: Qualquer incidente deve ser reportado imediatamente à equipe de TI e/ou ao responsável pela segurança da informação.

Resposta e Recuperação: A equipe de TI deve ter um plano documentado para responder a incidentes, incluindo isolamento do problema, análise forense e recuperação de dados.

Relato de Incidentes: Após a resolução do incidente, um relatório deve ser gerado para análise e revisão, visando a melhoria contínua das políticas de segurança.

- Política de backup e recuperação de desastres.

Frequência de Backup: Os dados críticos da empresa devem ser copiados diariamente, com backups semanais completos armazenados em local seguro.

Armazenamento de Backups: Os backups devem ser armazenados em um local físico separado e também em uma solução de armazenamento na nuvem para garantir redundância.

Testes de Restauração: Testes de restauração dos backups devem ser realizados trimestralmente para garantir que os dados possam ser recuperados de forma eficaz.

Documentação do Plano de Recuperação: Um plano de recuperação de desastres deve ser documentado, detalhando os procedimentos a serem seguidos em caso de perda de dados ou falha do sistema.