Políticas de Segurança da Informação

As políticas de segurança da informação têm como objetivo proteger os ativos informacionais da organização, assegurando confidencialidade, integridade e disponibilidade dos dados. Essas políticas estabelecem diretrizes para o acesso aos sistemas, uso de dispositivos e redes, resposta a incidentes e estratégias de backup, promovendo uma cultura organizacional voltada à prevenção de riscos e ao cumprimento de boas práticas.

1. Política de Acesso e Controle de Usuários

Esta política determina que todas as credenciais de acesso aos sistemas corporativos devem ser únicas e intransferíveis, sendo atribuídas de acordo com o cargo e função do colaborador. O objetivo é garantir a rastreabilidade e a responsabilização de ações realizadas nos sistemas.

Além disso, a autenticação de dois fatores (2FA) deve ser aplicada para todos os usuários que acessam dados sensíveis, aumentando a segurança contra acessos não autorizados. O controle de permissões deve obedecer ao princípio do menor privilégio, ou seja, os usuários devem ter acesso apenas às informações essenciais para o desempenho de suas atividades.

Contas inativas por mais de 30 dias serão automaticamente desativadas, e as senhas devem ser trocadas a cada 90 dias, prevenindo acessos indevidos. Essa política visa minimizar o risco de vazamentos e invasões, seja por falha humana ou por ações maliciosas.

2. Política de Uso de Dispositivos Móveis e Redes

A política estabelece que qualquer dispositivo utilizado para acessar a rede da empresa, seja corporativo ou pessoal autorizado (BYOD), deve contar com antivírus atualizado, bloqueio por senha e, sempre que possível, criptografia dos dados. Tais requisitos reforçam a proteção contra softwares maliciosos e acessos indevidos.

O acesso a redes Wi-Fi públicas será permitido somente mediante uso de VPN corporativa, assegurando a confidencialidade das informações transmitidas. O uso de dispositivos pessoais deve passar por aprovação prévia da equipe de TI, que será responsável pelo monitoramento e conformidade desses equipamentos.

Essa política tem como finalidade manter a segurança da informação fora do ambiente corporativo, prevenindo ataques externos e perdas de dados em dispositivos móveis.

3. Política de Resposta a Incidentes de Segurança

Todos os incidentes de segurança da informação devem ser comunicados imediatamente à equipe de TI, permitindo uma resposta ágil e eficaz. Após o reporte, será conduzida uma investigação para identificar a origem, impacto e alcance do incidente, com registro técnico de todas as etapas.

Medidas de contenção e correção serão aplicadas para mitigar danos e evitar reincidências. Além disso, treinamentos de conscientização sobre segurança da informação ocorrerão semestralmente, preparando os colaboradores para reconhecer e agir diante de ameaças.

O principal objetivo dessa política é garantir resiliência organizacional e redução dos impactos causados por falhas de segurança, promovendo uma resposta estruturada a incidentes.

4. Política de Backup e Recuperação de Desastres

Backups de todos os dados críticos da organização devem ser realizados diariamente e de forma automatizada, assegurando a integridade e disponibilidade das informações. As cópias de segurança devem ser armazenadas tanto localmente quanto em ambiente de nuvem seguro, diversificando os pontos de recuperação.

Testes de restauração serão realizados mensalmente para verificar a eficácia e a confiabilidade dos backups. O tempo máximo para recuperação dos sistemas (RTO – Recovery Time Objective) será de 24 horas, o que garante a continuidade das operações em caso de falhas, ataques cibernéticos ou desastres naturais.

Essa política tem como finalidade proteger a empresa contra perda de dados e paralisações operacionais, assegurando a continuidade dos serviços mesmo em situações críticas.