

Universidade São Judas Tadeu

Ciência da computação

Atividade Sistemas computacionais e segurança

Arthur Carvalho -825111150

Fabio Marano – 825124892

Leonardo Ferreira – 825124892

Lucas de Lima Garcia – 825145166

Matheus Fraga – 82425021

Matheus da Silva – 825144599

Thiago Carvalho - 825117520

Professor Orientador

Robson Calvetti

Desenvolvimento de Políticas de Segurança da Informação
Empresa Fictícia: TechMini
Curso de Ciência da Computação

1. Políticas de Acesso e Controle de Usuários

Objetivo:

Garantir que apenas usuários autorizados tenham acesso às informações e sistemas da empresa, de forma apropriada ao seu papel e responsabilidade.

Política Proposta:

- Cada colaborador terá um usuário e senha únicos, com autenticação de dois fatores (2FA) habilitada sempre que possível.
- O acesso será concedido com base no princípio do menor privilégio: os usuários terão acesso apenas ao que for essencial para suas funções.
- Contas inativas ou de ex-funcionários serão desativadas imediatamente após o desligamento.
- Haverá uma revisão de acessos a cada três meses para garantir que estejam atualizados e corretos.

Justificativa:

Essa política reduz o risco de acessos indevidos e dificulta ações maliciosas ou acidentais por parte de usuários não autorizados.

2. Política de Uso de Dispositivos Móveis e Redes

Objetivo:

Assegurar o uso seguro de dispositivos móveis e o acesso a redes internas e externas, minimizando os riscos de vazamento de dados ou acesso não autorizado.

Política Proposta:

- Dispositivos móveis utilizados para trabalho (incluindo celulares e notebooks pessoais) devem ter senha de acesso e estar protegidos com antivírus atualizado.
- O acesso remoto à rede da empresa será feito apenas por meio de VPN segura.
- É proibido o uso de redes Wi-Fi públicas para atividades corporativas

sem a proteção de VPN.

- O uso de dispositivos pessoais (BYOD - Bring Your Own Device) será permitido mediante autorização e com configurações de segurança exigidas.

Justificativa:

Essa política protege os dados da empresa mesmo quando os colaboradores estão fora do ambiente físico da organização.

3. Diretrizes para Resposta a Incidentes de Segurança

Objetivo:

Estabelecer um plano de ação rápido e eficaz diante de incidentes que envolvam segurança da informação, como ataques, vazamentos ou falhas.

Política Proposta:

- Qualquer suspeita de incidente deve ser imediatamente comunicada ao responsável técnico ou gestor da área.
- Um plano de resposta será acionado com as seguintes etapas: identificação, contenção, erradicação, recuperação e análise posterior.
- Todos os incidentes serão registrados, documentados e analisados para evitar recorrências.
- A empresa realizará simulações de resposta a incidentes periodicamente para treinar a equipe.

Justificativa:

Ter um protocolo claro reduz o tempo de resposta, limita os danos e mostra maturidade organizacional.

4. Política de Backup e Recuperação de Desastres

Objetivo:

Assegurar a integridade e disponibilidade dos dados da empresa, mesmo em caso de falhas técnicas, desastres naturais ou ataques virtuais.

Política Proposta:

- Backups completos serão realizados semanalmente e backups incrementais diariamente.
- Os dados serão armazenados em três cópias: uma local, uma em servidor externo e uma em nuvem.
- Todos os backups serão criptografados e testados mensalmente quanto à integridade e capacidade de restauração.
- Será criado um plano de recuperação de desastres com papéis bem definidos e tempo estimado de recuperação (RTO) de até 24 horas.

Justificativa:

A política de backup garante que informações cruciais possam ser recuperadas, assegurando continuidade e confiabilidade nos serviços.

Conclusão

Essas políticas foram elaboradas pensando na realidade de pequenas empresas, que muitas vezes não possuem grandes recursos, mas precisam garantir a segurança de suas operações. Com medidas simples, bem definidas e implementadas com disciplina, é possível proteger a empresa contra ameaças e imprevistos, garantindo um ambiente mais seguro e profissional para todos.