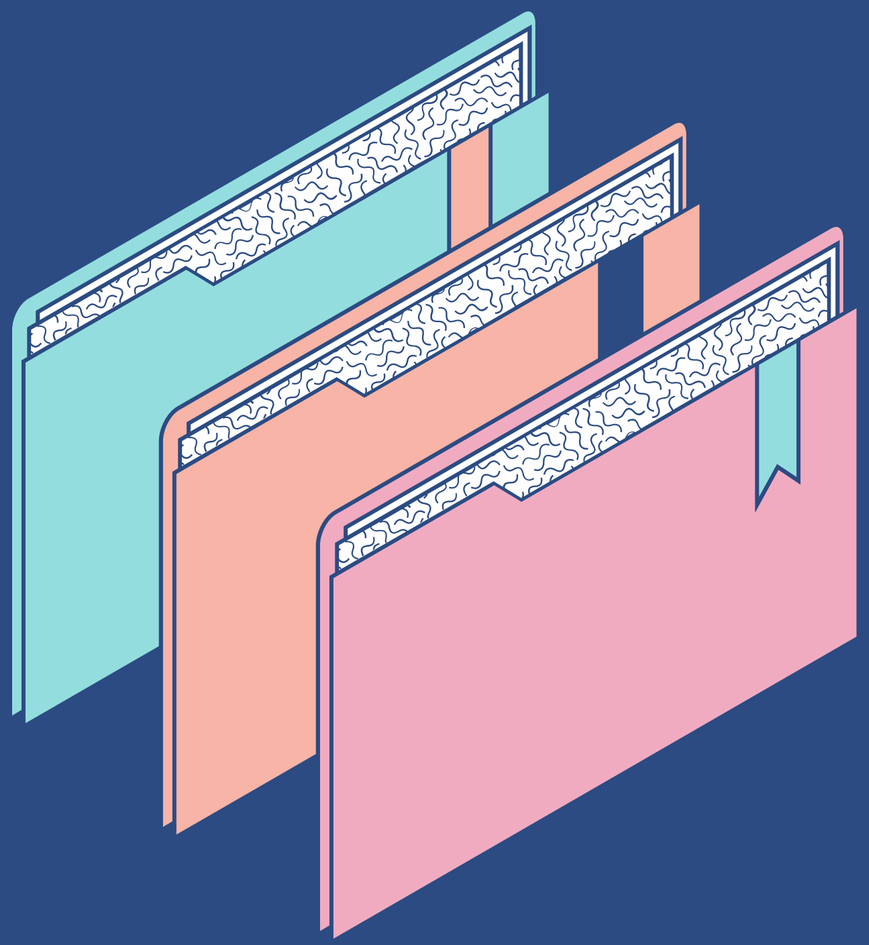
Desenvolvimento de Políticas de Segurança para uma Pequena Empresa



Políticas de Acesso e Controle de Usuários Controle de acesso

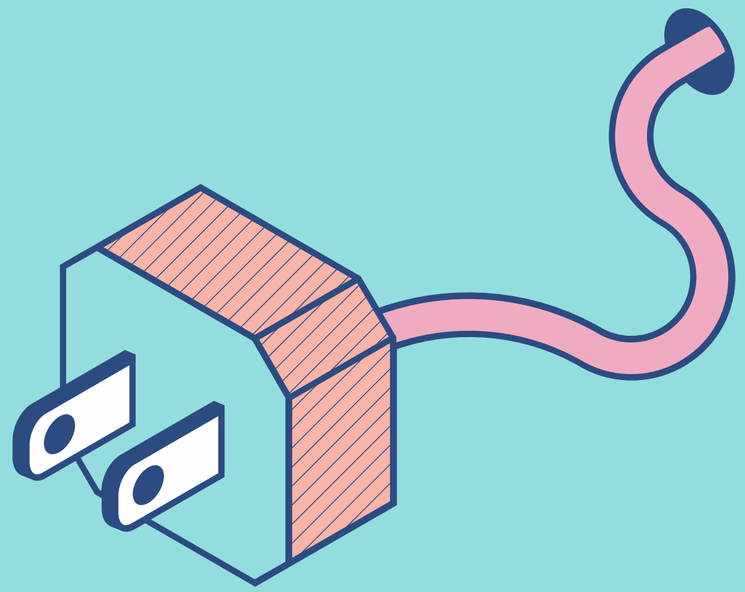
- Políticas de Acesso e Controle de Usuários Controle de acesso é crucial para proteger dados e ativos.
- Segurança da informação deve ser garantida em todos os níveis organizacionais.
- Define como funcionários acessam sistemas e informações.

Regras de Acesso e Controle

Criação e gerenciamento de contas devem ser centralizados e autorizados.

Senhas complexas e MFA ajudam a evitar acessos não autorizados.

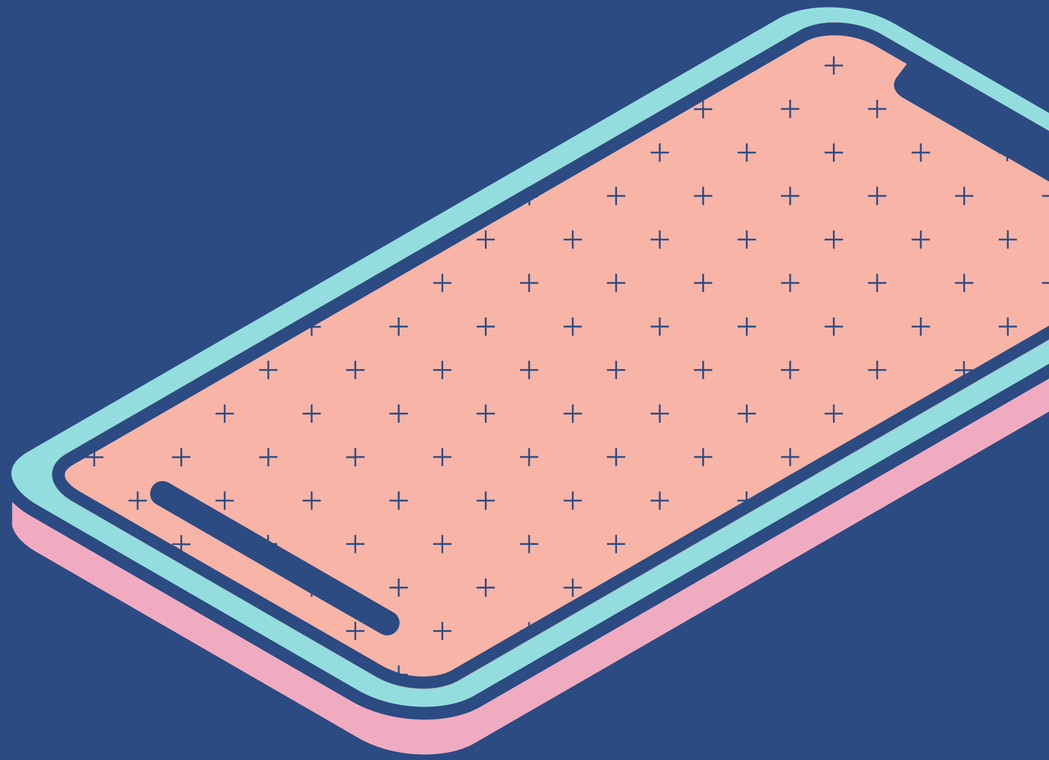
Auditorias regulares de permissões para garantir conformidade.



Controle e Monitoramento

- Somente pessoal autorizado pode acessar áreas críticas físicas e virtuais.
- Logs de acesso são registrados e analisados periodicamente para identificar anomalias.
- Acesso remoto deve ser realizado através de VPN segura, garantindo segurança adicional.

Política de Uso de Dispositivos Móveis



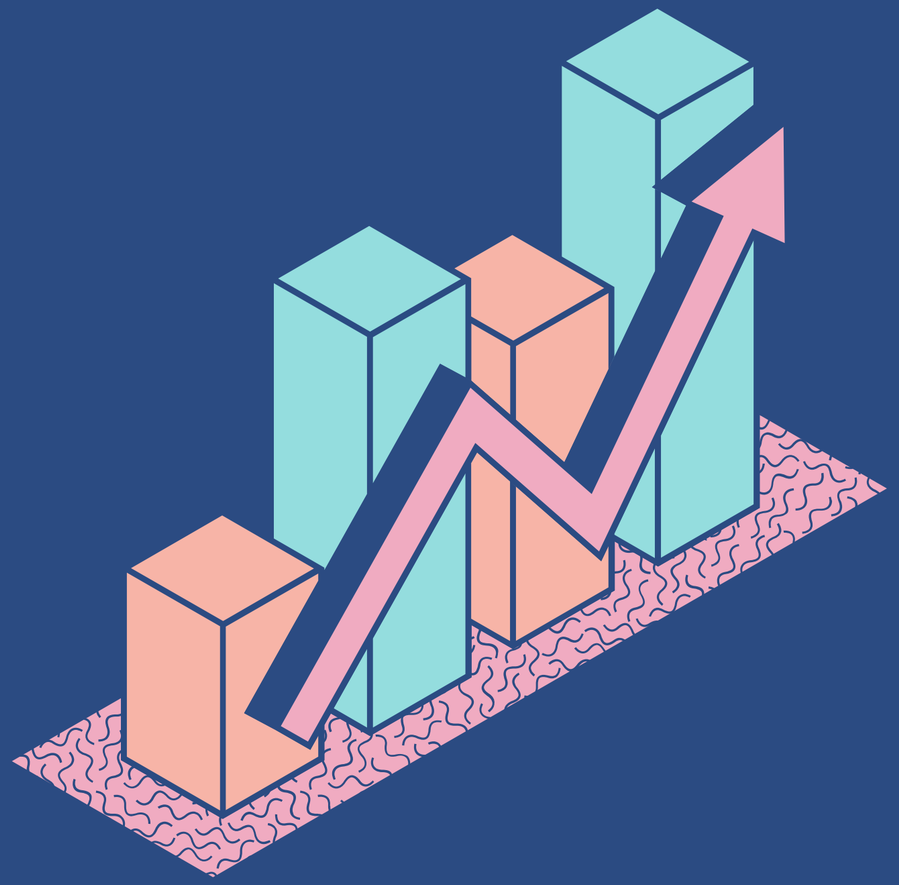
Dispositivos móveis devem ser utilizados exclusivamente para fins corporativos.
Uso para fins pessoais é estritamente proibido para evitar vulnerabilidades e perda de dados.
Proteger dispositivos móveis com criptografia e bloqueios de tela é fundamental.

Boas Práticas de Uso

O usuário é responsável pela boa conservação dos dispositivos fornecidos pela empresa.

Equipamentos devem ser protegidos contra roubo, perda ou danos, e devolvidos em bom estado ao término do contrato.

Evitar salvar arquivos no dispositivo e utilizar armazenamento na rede corporativa.



Restrições e Monitoramento

- Uso dos dispositivos não é permitido no horário de trabalho, salvo exceções aprovadas.

- Navegação em sites impróprios ou não relacionados às atividades laborais é proibida.

- A empresa monitora o uso de dispositivos e redes para garantir conformidade com as políticas.

Diretrizes para Resposta a Incidentes de Segurança

Preparação:

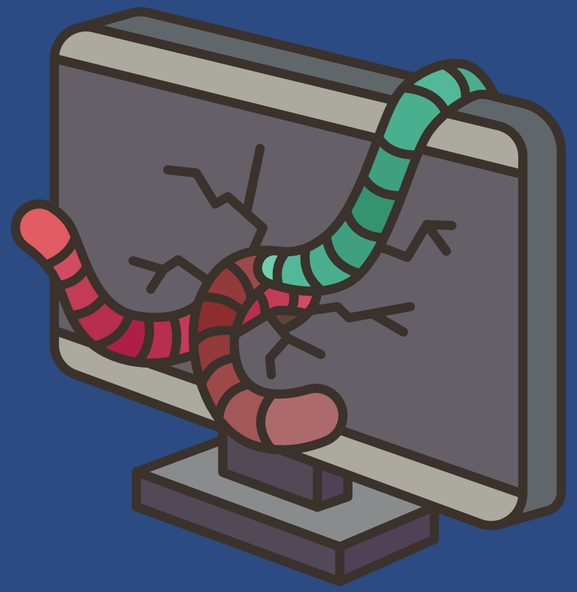
Treinamento da equipe utilizando de ferramentas adequadas para obter uma resposta eficiente.

Identificação:

Incidentes devem ser detectados rapidamente para minimizar impactos.

Contenção:

Ação rápida para isolar a ameaça e impedir sua propagação.



Erradicação:

Erradicação nada mais é que a identificação da causa raiz do incidente e remoção das ameaças associadas

Recuperação:

E a recuperação se trata de restaurar os sistemas afetados e garantir que estejam protegidos contra novos incidentes.

Verificação de que o sistema está seguro antes de voltar ao uso normal.

Aprendizado e Melhoria Contínua

Realizar uma análise detalhada após o incidente para identificar melhorias.

Atualizar as políticas de segurança e treinar a equipe com base nas lições aprendidas.

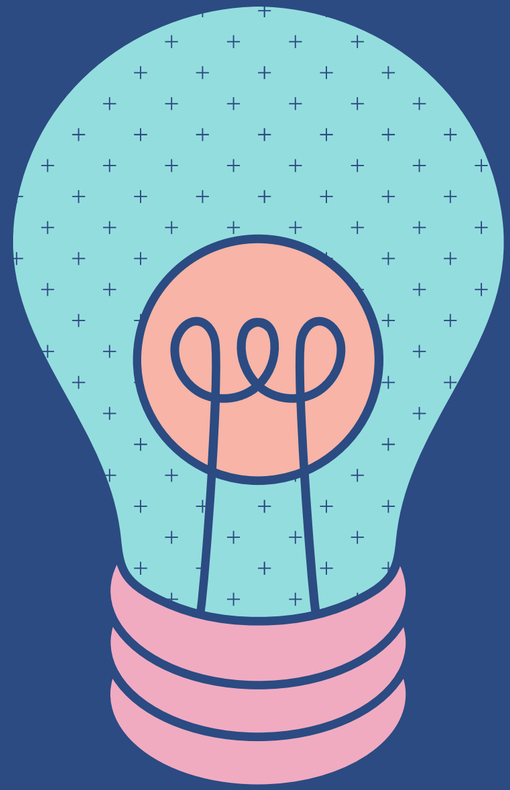
Registros detalhados ajudam a identificar tendências e ajustar respostas futuras.

Importância de Backup

O backup é a base da proteção de dados contra perda acidental, falhas de hardware ou ciberataques.

Reduz os impactos de desastres e garante a continuidade das operações.

Backup regular é uma parte crítica da estratégia de segurança.

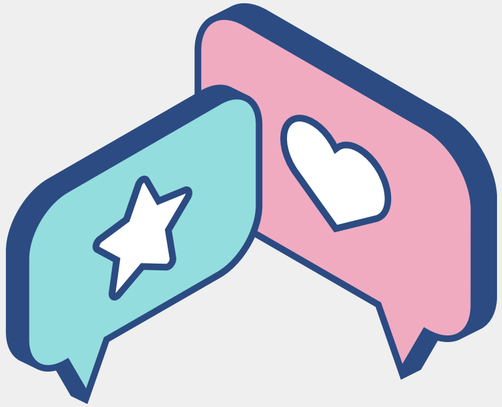


Regras de Backup

Backup completo deve ser realizado semanalmente e backups incrementais diários.

Dados devem ser armazenados em locais seguros, com cópias off-site para maior segurança.

Política de retenção de dados: backups devem ser mantidos por um período definido.



Plano de Recuperação de Desastres

- Estratégias de recuperação incluem identificar sistemas críticos para recuperação prioritária.
- Testes periódicos do plano de recuperação garantem que a equipe está preparada para desastres.
- Revisão contínua do plano com base em mudanças no ambiente e novas ameaças.

OBRIGADO POR ASSISTIREM!

MATHEUS BOVO- 824138656

RAFAEL CEZAR- 82425725

FELIPE GATTI- 824125546

WESLEY DOS SANTOS- 82422607

ITALO GOMES- 824218750