Políticas de Segurança para uma Pequena Empresa

Soluções Computacionais e Segurança

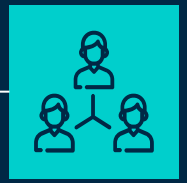
Integrantes

Ana Carolina dos Reis Ramos	82413448
Ana Luisa Martins Da Silva	824219533
Gustavo Leal de Almeida	824138271
Matheus Moniakas	82422355
Milena	824213909
Murilo Passos	824217071
Paulo Passiano	824219946

Introdução

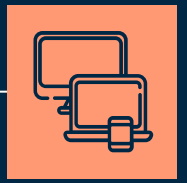
O nosso trabalho é composto por um conjunto prático de políticas de Segurança da Informação para uma escola particular fictícia, com foco em proteger os seus ativos digitais, dados confidenciais de alunos, funcionários e setores internos da escola, bem como assegurar a continuidade de suas operações.

Tópicos



01

Políticas de Acesso e Controle de Usuários



02

Políticas de Uso de Dispositivos Móveis e Redes

03

Diretrizes para Respostas a Incidente de Segurança

04

Política de Backup e Recuperação de Desastres

Políticas de Acesso e Controle de Usuários

01

Políticas de Acesso e Controle de Usuários

- **Autenticação de Usuários**
  - Todos os usuários, incluindo funcionários, professores, administradores e alunos, devem se autenticar para acessar qualquer sistema de TI da escola, seguindo práticas seguras para a criação de credenciais.
    Exemplo de senha: A@scHoOl2023!

  - Para acesso a informações confidenciais como dados médicos de alunos ou registros financeiros, será obrigatória a **Autenticação Multifator (MFA)** , utilizando métodos como *tokens* de autenticação, códigos enviados por SMS ou apps de autenticação.

Políticas de Acesso e Controle de Usuários

- **Gerenciamento de Privilégios e Segregação de Funções**
  - Todos os usuários devem ser categorizados em grupos funcionais com níveis de privilégio específicos. O uso do princípio do **Menor Privilégio** é imperativo. Um funcionário só deve ter o nível de acesso necessário para cumprir suas tarefas.

    Exemplo: Professores terão acesso restrito às informações acadêmicas dos alunos sob sua responsabilidade, mas não terão acesso a dados financeiros.

Políticas de Acesso e Controle de Usuários

- **Monitoramento de Acessos**
  - O setor de TI deverá registrar toda tentativa de acesso aos sistemas críticos. Em caso de atividades suspeitas, um alerta automático será enviado à administração da escola.

    – Logs de acesso

    – Falhas de login

    – Tentativas atípicas de acessos

Políticas de Uso de Dispositivos Móveis e Rede

02

Políticas de Uso de Dispositivos Móveis e Redes

- **Dispositivos Móveis Pessoais – BYOD Bring Your Own Device**
  - A escola permite que funcionários e professores usem seus próprios dispositivos móveis para fins de trabalho, desde que sigam regras rigorosas de segurança. Sendo elas:

    - Dispositivos devem ser criptografados para proteger dados sensíveis armazenados localmente.

    - Devem ter antivírus e software de segurança atualizado instalado.

    - O uso de VPN para acessos à sistemas da escola.

Políticas de Uso de Dispositivos Móveis e Redes

- **Uso Seguro da Rede WI-FI**
  - A rede WI-FI da escola será segregada em grupos:

    - **Rede Administrativa:** De uso exclusivo da administração, com criptografia WPA3 e monitoramento constante do tráfego. Apenas dispositivos autorizados podem se conectar a essa rede.

    - **Rede Educacional:** Usada por professores e alunos para atividades acadêmicas, com controle de banda e filtros de conteúdo para evitar o uso inadequado.

    - **Rede de Visitantes:** Disponível para convidados e prestadores de serviços, com um tempo limitado de acesso e sem conexão direta a sistemas críticos da escola.

    - **Rede Estudantil:** De uso exclusivo dos alunos para acesso aos sistemas de notas, com controle de banda e filtros de conteúdo para evitar o uso inadequado.

Políticas de Uso de Dispositivos Móveis e Redes

- **Monitoramento de Rede e Uso de Internet**
  - A equipe de TI deve utilizar ferramentas de monitoramento de rede para identificar tráfego anormal, tentativas de acesso não autorizado e violações das políticas de uso da Internet

    Exemplo: Download de *software* não autorizado.

Diretrizes para Respostas a Incidentes de Segurança

03

Diretrizes para Respostas a Incidentes de Segurança

- **Plano de Respostas a Incidentes PRI**
  - A escola deverá criar e manter um **Plano de Resposta a Incidentes (PRI)** detalhado. O PRI irá conter:

    – Identificação de possíveis incidentes, como ataques de *ransomware*, violações de dados, falhas sistêmicas.

    – Procedimentos para contenção rápida do incidente, como desconectar sistemas afetados da rede.

    – Notificação das partes interessadas, como a direção da escola, alunos e pais.

    – Análise pós-incidente para identificar vulnerabilidades exploradas e planejar melhorias.

Diretrizes para Respostas a Incidentes de Segurança

- **Equipe de Resposta a Incidentes**
  - Será designada uma equipe de resposta composta por membros da TI, administradores e, se necessário, consultores externos de segurança. Cada incidente deverá ser escalado conforme sua gravidade, e a equipe deverá agir conforme as diretrizes do PRI.

- **Notificações e Relatórios**
  - Todos os incidentes devem ser registrados em relatórios detalhados, incluindo as ações tomadas e o tempo de resposta. A escola deve informar os alunos e pais em caso de vazamento de dados pessoais.

Política de Backup e Recuperação de Desastres

04

Política de Backup e Recuperação de Desastres

- **Backup Diário e Incremental**
  - A escola deve realizar backups completos de todos os dados sensíveis, incluindo registros acadêmicos, financeiros e de saúde, diariamente, tanto localmente quanto em servidores na nuvem.

  - Backups incrementais, apenas dos dados alterados, serão realizados a cada hora para reduzir a janela de perda de dados.

Política de Backup e Recuperação de Desastres

- **Armazenamento de Backups em Locais Seguros**
  - Os backups serão armazenados em dois locais distintos: um backup local criptografado e um backup em nuvem, para garantir redundância e recuperação em caso de desastre físico (como incêndios ou inundações).

    Exemplo: Se os servidores locais da escola forem comprometidos por um ataque de *ransomware*, os dados poderão ser restaurados rapidamente a partir da cópia armazenada na nuvem.

Política de Backup e Recuperação de Desastres

- **Teste de Recuperação Regulares**
  - A escola deverá testar sua capacidade de restaurar dados a partir dos backups pelo menos uma vez por trimestre. Os testes ajudarão a identificar problemas no processo de recuperação antes que um incidente ocorra.
- **Plano de Recuperação de Desastres**
  - O PRD irá detalhar os procedimentos para restaurar as operações da escola em caso de catástrofe, como um incêndio que destrua a infraestrutura local. O plano incluirá o tempo máximo aceitável para recuperação **(RTO – Recovery Time Objective)** e o volume máximo de dados que pode ser perdido sem grandes impactos **(RPO – Recovery Point Objective).**

Conclusão

A implementação adequada dessas políticas garantirá que a instituição esteja preparada para enfrentar ameaças internas e externas, proteger seus dados e manter a continuidade das operações.

Obrigada pela Atenção