Política de Monitoramento de Segurança para o Setor de Educação

Baseado no Framework NIST 800-53 (RMF)

2. Propósito

Estabelecer um processo contínuo para monitorar e detectar atividades anormais e potenciais ameaças em sistemas de informação e ativos de informação do setor de educação, a fim de proteger a confidencialidade, integridade e disponibilidade de dados críticos e sistemas educacionais.

3. Escopo

Esta política se aplica a todos os sistemas de informação e ativos de informação do setor de educação, incluindo:

- **Redes:** Redes de computadores, incluindo redes administrativas, redes de ensino e redes de alunos.
- **Dispositivos:** Computadores, servidores, dispositivos móveis, tablets e outros dispositivos conectados.
- **Aplicações:** Softwares e aplicações utilizados para ensino, administração e pesquisa.
- **Dados:** Informações confidenciais dos alunos, dados de funcionários, registros financeiros e dados de pesquisa.

4. Política

O setor de educação se compromete a:

- **Monitorar continuamente os sistemas de informação:** Implementar ferramentas e técnicas de monitoramento para detectar atividades anormais e potenciais ameaças em tempo real.
- **Detectar e responder a incidentes de segurança:** Identificar rapidamente incidentes de segurança e tomar medidas para conter o dano e restaurar a operação normal dos sistemas.
- **Analisar eventos de segurança:** Investigar eventos de segurança para determinar a causa raiz e tomar medidas para prevenir futuros incidentes.
- **Relatar eventos de segurança:** Notificar as autoridades competentes sobre eventos de segurança relevantes de acordo com os procedimentos estabelecidos.

5. Procedimentos Relacionados

- **Monitoramento de rede:**
  - Monitorar o tráfego de rede para detectar atividades anormais e potenciais ataques.
  - Implementar sistemas de detecção de intrusão (IDS) e sistemas de prevenção de intrusão (IPS).
- **Monitoramento de dispositivos:**
  - Monitorar os dispositivos para detectar atividades anormais e potenciais malwares.
  - Implementar software de antivírus e antimalware em todos os dispositivos.
- **Monitoramento de aplicações:**
  - Monitorar as aplicações para detectar atividades anormais e potenciais vulnerabilidades.
  - Implementar testes de penetração e avaliações de segurança de aplicações.
- **Análise de eventos de segurança:**

    - Investigar eventos de segurança para determinar a causa raiz e o impacto potencial.
    - Identificar as medidas necessárias para remediar o incidente e prevenir futuros eventos.
- **Relato de eventos de segurança:**
    - Notificar as autoridades competentes sobre eventos de segurança relevantes de acordo com os procedimentos estabelecidos.
    - Documentar todos os eventos de segurança e as medidas tomadas para remediá-los.

6. Não Conformidade

O não cumprimento desta política poderá resultar em medidas disciplinares, incluindo advertência verbal, advertência escrita, suspensão ou rescisão de contrato.

7. Compromisso/Autoridade da Gestão

A alta gerência do setor de educação se compromete a fornecer os recursos necessários para a implementação e o cumprimento desta política. A equipe de segurança da informação é responsável pela gestão e atualização da política.

8. Cronograma de Revisão

A política será revisada anualmente ou após um incidente de segurança cibernética significativo.

9. Definições

- **Monitoramento de segurança:** Processo de coleta e análise de informações de segurança para detectar atividades anormais e potenciais ameaças.
- **Incidente de segurança:** Evento que pode causar perda de confidencialidade, integridade ou disponibilidade dos sistemas de

informação ou dos dados.

- **Análise de eventos de segurança:** Processo de investigação de um incidente de segurança para determinar a causa raiz e o impacto potencial.
- **Relato de eventos de segurança:** Processo de notificação das autoridades competentes sobre um incidente de segurança.

Observações:

- Esta política é um exemplo e deve ser adaptada às necessidades específicas do setor de educação.
- É importante consultar especialistas em segurança cibernética para a implementação da política.