Desafio para Elaboração de uma Política de Segurança da Informação (PSI) em um Ambiente Hospitalar

Desafio:

Você foi contratado como consultor de segurança da informação por um hospital de grande porte. Sua missão é desenvolver uma Política de Segurança da Informação (PSI) que garanta a proteção dos dados sensíveis dos pacientes, a integridade dos sistemas de TI e a conformidade com regulamentos de privacidade e segurança, como a LGPD (Lei Geral de Proteção de Dados) no Brasil.

Requisitos do Desafio:

1. Avaliar o Ambiente:
- Realize um levantamento detalhado dos ativos de informação do hospital, incluindo sistemas de TI, bases de dados, dispositivos médicos conectados à rede e documentos físicos.
- Identifique possíveis ameaças e vulnerabilidades que podem afetar a segurança dos dados e sistemas.

2. Definir Objetivos da PSI:
- Assegurar a confidencialidade, integridade e disponibilidade das informações dos pacientes.
- Cumprir com a LGPD e outras regulamentações relevantes.
- Minimizar riscos de ataques cibernéticos e incidentes de segurança.

3. Desenvolver Políticas e Procedimentos:
- Elabore políticas e procedimentos claros e específicos para proteger os ativos de informação.
- Inclua diretrizes para o uso de dispositivos móveis, acesso remoto, senhas, e-mails e redes sociais.

4. Treinamento e Conscientização:
- Crie um programa de treinamento para todos os funcionários do hospital sobre as políticas de segurança da informação.
- Desenvolva campanhas de conscientização contínuas para reforçar a importância da segurança da informação.

5. Implementação e Monitoramento:
- Estabeleça um plano de implementação das políticas e procedimentos.
- Defina métricas e processos de monitoramento para garantir a eficácia da PSI.

Exemplo de Política de Segurança da Informação para um Ambiente Hospitalar

---

Política de Segurança da Informação (PSI) do Hospital ABC

1. Introdução

A Política de Segurança da Informação (PSI) do Hospital ABC tem como objetivo proteger as informações sensíveis dos pacientes, garantir a integridade dos sistemas de TI e assegurar a conformidade com a LGPD e outras regulamentações aplicáveis.

2. Objetivos

- Proteger a confidencialidade, integridade e disponibilidade das informações dos pacientes.
- Assegurar o cumprimento da LGPD e outras regulamentações de privacidade e segurança.
- Reduzir os riscos de ataques cibernéticos e incidentes de segurança.

3. Levantamento de Ativos de Informação

- Sistemas de TI: Prontuários eletrônicos, sistemas de gestão hospitalar, bases de dados.
- Dispositivos Médicos: Equipamentos conectados à rede, como monitores de sinais vitais.
- Documentos Físicos: Fichas de pacientes, relatórios médicos.
- Outros: Dispositivos móveis, laptops, redes Wi-Fi.

4. Políticas e Procedimentos

4.1 Uso de Dispositivos Móveis e Acesso Remoto

- Todos os dispositivos móveis devem ter criptografia habilitada.
- O acesso remoto aos sistemas hospitalares só será permitido por meio de VPN segura.
- Senhas fortes e autenticação de dois fatores são obrigatórios.

4.2 Senhas

- Senhas devem ter no mínimo 8 caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais.
- Senhas devem ser alteradas a cada 90 dias.
- É proibido compartilhar senhas.

4.3 E-mails e Redes Sociais

- É proibido enviar informações sensíveis de pacientes por e-mail sem criptografia.
- Funcionários não devem postar informações relacionadas a pacientes ou procedimentos hospitalares em redes sociais.

5. Treinamento e Conscientização

- Todos os funcionários devem participar de treinamentos anuais sobre segurança da informação.
- Campanhas de conscientização serão realizadas periodicamente para reforçar a importância da PSI.

6. Implementação e Monitoramento

- Um plano de implementação será desenvolvido, detalhando as etapas necessárias para colocar a PSI em prática.
- Serão estabelecidas métricas para monitorar a conformidade e a eficácia da PSI.
- Auditorias internas serão realizadas semestralmente para garantir a aderência às políticas e procedimentos.

7. Conformidade e Penalidades

- O não cumprimento desta PSI pode resultar em ações disciplinares, incluindo advertências, suspensão ou demissão, conforme a gravidade da infração.

8. Revisão da PSI

- Esta PSI será revisada anualmente ou sempre que houver mudanças significativas na legislação ou nos procedimentos internos do hospital.

Conclusão

A elaboração de uma Política de Segurança da Informação eficaz é crucial para proteger os dados sensíveis em um ambiente hospitalar. Seguindo as etapas e diretrizes apresentadas, o Hospital ABC estará melhor preparado para enfrentar desafios de segurança e garantir a conformidade com as regulamentações vigentes.