A LGPD e a Segurança da Informação

Protegendo dados de pacientes e alunos

Introdução

A segurança da informação tem se tornado uma preocupação crescente em todas as esferas da sociedade, especialmente em instituições que lidam com dados sensíveis, como hospitais e universidades. A **Fundação Educacional D André Arcoverde (FAA),** que abrange a **UNIFAA**, dois hospitais, além de outras mantidas, encara esses desafios, buscando implementar rigorosos protocolos para proteger as informações de seus pacientes e alunos. Com a **Lei Geral de Proteção de Dados** (**LGPD**) no Brasil, a necessidade de garantir a confidencialidade, integridade e disponibilidade dos dados tornou-se ainda mais relevante.

Este artigo explora a importância da **LGPD**, detalha as ameaças que golpistas representam ao tentar acessar dados de pacientes e alunos, e oferece estratégias para prevenir vazamentos de informações. Além disso, analisamos cenários específicos de segurança que a **FAA** poderia enfrentar, ilustrando com exemplos práticos de incidentes. A meta é fortalecer a conscientização sobre a proteção de dados e destacar as medidas que podem ser adotadas para mitigar riscos, assegurando que a instituição continue a cumprir seu papel com segurança e responsabilidade.

O que é a LGPD?

A **Lei Geral de Proteção de Dados Pessoais (LGPD)**, Lei **nº 13.709/2018**, é a legislação brasileira que regula as atividades de tratamento de dados pessoais. A **LGPD** visa proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A lei estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo penalidades significativas para as instituições que não cumprirem suas diretrizes.

Por que seguir a LGPD é relevante para instituições como a FAA?

Instituições educacionais e de saúde, como a **FAA**, a conformidade com a **LGPD** é extremamente relevante por várias razões:

1. **Proteção dos Direitos dos Indivíduos**: A **LGPD** assegura que os dados pessoais sejam tratados com ética e segurança, protegendo a privacidade dos indivíduos.
2. **Segurança e Confiança**: Manter a segurança dos dados fortalece a confiança dos pacientes e alunos na instituição.
3. **Prevenção de Penalidades Legais**: O descumprimento da **LGPD** pode resultar em multas significativas e sanções administrativas.
4. **Mitigação de Riscos**: Medidas de conformidade reduzem a probabilidade de vazamentos e outros incidentes de segurança.
5. **Melhoria na Governança de Dados**: Promove a transparência e responsabilidade no tratamento de informações, otimizando processos internos.
6. **Vantagem Competitiva**: A conformidade com a **LGPD** pode ser um diferencial significativo, atraindo alunos, pacientes e parceiros.
7. **Responsabilidade Social**: Reflete um compromisso ético com a sociedade, garantindo o tratamento seguro dos dados.

Seguir a **LGPD** é fundamental para a **FAA** continuar a fornecer serviços de alta qualidade, mantendo a integridade e a confiança da comunidade que atende.

Desafios e impactos das violações de dados na área da saúde

Os desafios enfrentados pelas instituições de saúde estão associados a um momento de alta complexidade e vulnerabilidade. Atualmente, **93%** das instituições de saúde sofreram violações de dados nos últimos dois anos. Dessas instituições, **43%** enfrentaram tempo de inatividade operacional como consequência, resultando em atrasos no atendimento ao paciente, impactos negativos na receita e queda na satisfação dos profissionais de saúde.

Um incidente notável foi o do **Conecte SUS**, que apresentou falhas três meses após um ataque hacker que removeu informações críticas sobre notificações de casos, dados e mortes relacionadas à pandemia de **COVID-19**.

Em **2023**, o custo médio de uma violação de dados atingiu um recorde de **US$ 4,45 milhões**, de acordo com a **IBM** e o Instituto **Ponemon**, representando um aumento de **2%** em comparação com **2022**, quando o custo era de **US$ 4,35 milhões**.

Esses números ressaltam a urgência de implementar medidas robustas de segurança da informação, especialmente em instituições que lidam com dados sensíveis, como hospitais e universidades.

Como golpistas podem conseguir os dados de pacientes e alunos?

Golpistas utilizam diversas técnicas para obter dados sensíveis, entre as mais comuns estão:

1. **Engenharia Social**: Manipulação psicológica para enganar as pessoas a revelar informações confidenciais. Isso pode incluir ligações falsas, utilização de redes sociais, ou até interações presenciais.
2. **Phishing**: Envio de e-mails ou mensagens que parecem ser de fontes confiáveis para induzir o destinatário a fornecer informações pessoais.
3. **Acesso Físico Não Autorizado**: Golpistas podem tentar acessar fisicamente áreas restritas onde dados são armazenados, como secretarias ou UTIs.
4. **Interceptação de Comunicações**: Golpistas podem interceptar comunicações eletrônicas não criptografadas para obter dados sensíveis.

O que golpistas podem fazer com esses dados?

Com acesso a dados pessoais e sensíveis, golpistas podem:

1. **Extorsão**: Utilizar informações sensíveis para chantagear pacientes ou alunos, exigindo pagamento para não divulgar informações privadas.
2. **Roubo de Identidade**: Utilizar informações pessoais para abrir contas bancárias, solicitar empréstimos ou realizar compras fraudulentas.
3. **Vendas de Dados**: Vender informações obtidas para outros criminosos ou organizações ilegais.

Formas de evitar e se proteger de vazamentos

Para prevenir vazamentos de dados, devemos adotar as seguintes medidas:

1. **Treinamento e Conscientização**: Participar dos treinamentos disponibilizados sobre práticas seguras de manuseio de dados e como reconhecer tentativas de phishing e engenharia social.
2. **Políticas de Segurança**: Seguir as políticas de controle de acesso, tanto físico quanto digital, garantindo que apenas pessoal autorizado possa acessar dados sensíveis.
3. **Criptografia de Dados**: Utilizar criptografia para proteger dados armazenados e transmitidos, tornando-os ilegíveis para qualquer pessoa não autorizada a acessá-los.
4. **Auditorias Regulares**: Colaborar nas auditorias de segurança para identificar e corrigir vulnerabilidades.

Impactos de vazamentos de dados

Os vazamentos de dados podem ter consequências graves para a instituição, pacientes e alunos:

1. **Impactos para a Instituição**:
    - **Financeiros**: Multas significativas e custos com processos judiciais.
    - **Reputação**: Danos à reputação podem resultar na perda de confiança dos pacientes, alunos e do público em geral.
    - **Operacionais**: Tempo e recursos necessários para lidar com o vazamento podem afetar as operações diárias.
2. **Impactos para Pacientes e Alunos**:
    - **Privacidade**: Exposição de informações pessoais e médicas sensíveis.
    - **Segurança Pessoal**: Risco de extorsão e chantagem.
    - **Estresse Emocional**: Ansiedade e preocupação decorrentes da violação de privacidade.

Possíveis cenários de violações segurança

***Cenário 1**: Ligações Externas ao Hospital*

Situação: Golpistas ligam para o hospital, se passando por médicos ou representantes de órgãos reguladores, e solicitam dados de pacientes da **UTI**. Com essas informações, entram em contato com os familiares dos pacientes para extorsão.

Exemplo de Incidente: Em uma situação que poderia ser real, um golpista ligou para o hospital se passando por um médico da **UTI**, solicitando informações detalhadas sobre o estado de saúde de um paciente. Com os dados obtidos, o golpista contatou a família do paciente, alegando que um procedimento urgente e caro precisava ser realizado, exigindo um pagamento imediato.

***Cenário 2**: Ligações Externas à Universidade*

Situação: Golpistas ligam para a secretaria de uma instituição ensino, solicitando dados de alunos de medicina, e utilizam essas informações para criar situações de extorsão.

Exemplo de Incidente: Um golpista ligou para a secretaria de uma universidade, se passando por um representante do **MEC**, solicitando dados de contato de alunos de medicina sob o pretexto de uma pesquisa. Utilizando os dados obtidos, o golpista entrou em contato com os alunos, alegando ser de uma instituição de crédito estudantil e exigindo pagamentos indevidos.

Conclusão

A proteção dos dados de pacientes e alunos é essencial para a integridade e confiança da **FAA**. Implementar medidas de segurança robustas, conscientizar os colaboradores e realizar auditorias regulares são passos fundamentais para evitar possíveis vazamentos de dados e minimizar os impactos negativos. A conformidade com a **LGPD** não só protege a instituição contra penalidades, mas também fortalece a confiança e segurança de todos os envolvidos, contribuindo, junto de outros fatores, para a perenidade de nossa instituição.