

Rafael Santos

Especialista em Segurança da Informação Sênior

Brasília, DF

Com 7 anos de experiência em segurança cibernética, especializado em proteção de dados para empresas de tecnologia e instituições públicas. Certificado CISSP e CEH, com histórico de prevenção de mais de 200 ataques de ransomware e vazamento de dados.

HABILIDADES

Segurança de aplicações



Gestão de vulnerabilidades



Criptografia



SIEM



Pentest



LGPD



Firewall



Resposta a incidentes



PROJETOS EM DESTAQUE

LGPD Fintech X

Implementação de programa completo de conformidade com a LGPD incluindo mapeamento de dados, políticas de privacidade e treinamento desde a avaliação inicial até a auditoria da ANPD.

Resultados do projeto

- Zero vazamentos de dados em 2 anos de implementação
- Redução de 72% no número de vulnerabilidades de segurança
- Aprovação em auditoria da ANPD sem ressalvas

Segurança Hospitalar DF

Implementação de sistema de detecção de intrusão e monitoramento do Distrito Federal, protegendo dados de pacientes sensíveis.

Resultados do projeto

- Redução de 89% no número de incidentes de segurança
- Detecção de 15 tentativas de ataque de ransomware antes que causassem danos
- Economia de R\$ 1,8 milhões em possíveis multas por vazamento de dados

ARTIGOS

Conformidade com LGPD não é só burocracia: como ela protege os usuários e a sua empresa

Muitas empresas ainda veem a conformidade com a LGPD como um custo e não trazem retorno, mas essa visão é completamente equivocada. Quando falamos de Fintech X, um dos maiores benefícios que percebemos foi a redução das tentativas de ataque de ransomware que antes aconteciam 3 a 4 vezes por ano, e agora não acontecem nenhuma vez.

Outro ponto importante é que a conformidade com a LGPD aumenta a confiança dos usuários. Um exemplo que fizemos com os usuários da fintech depois da implementação mostrou

empresa por saber que seus dados estão protegidos. Um erro comum que a LGPD não trata como conformidade com LGPD como responsabilidade só do time de jurídico ou de segurança, mas sim um esforço de toda a empresa: desde o time de produto, que precisa projetar funcionalidades necessárias, até o time de marketing, que não pode usar dados de usuários sem a devida autorização.

No projeto dos hospitais públicos do DF, além de implementar as ferramentas de segurança em todos os colaboradores, desde médicos até pessoal da limpeza, sobre a implementação de uma política de segurança o resultado foi que a quantidade de incidentes causados por erro humano dos colaboradores é tão importante quanto as ferramentas de segurança.

Proteção de dados sensíveis na saúde: lições do projeto Segurança Hospitalar DF

Os dados de pacientes são alguns dos dados mais sensíveis que existem para as pessoas, além de muitas milionárias para as instituições de saúde. Na rede de hospitais públicos do DF, nosso maior desafio era proteger esses dados. Proteger os dados dos pacientes, que é uma atividade que não pode parar.

A primeira medida que tomamos foi implementar um sistema de monitoramento em tempo real, como tentativas de acesso a prontuários de pacientes por exemplo. Além disso, implementamos a criptografia de todos os dados armazenados, tanto nos servidores quanto nos dispositivos dos médicos e enfermeiros.

Outro ponto importante foi o treinamento de todos os colaboradores, que é fundamental para a informação e proteção de dados de pacientes. O resultado foi que a quantidade de incidentes caiu de 3 por mês para 1 por mês, e detectamos 15 tentativas de ataque de ransomware em nossos sistemas. A economia gerada pela prevenção de multas e danos foi de R\$ 1 milhão.