

ESTUDO DE CASO PCI Data Security Standard (PCI DSS)



A CSU Cardsystem S.A. é um processador de emissor e adquirente que realiza serviços de processamento de dados para pagamentos eletrônicos.



Qual programa sua empresa implementou para ajudar a endereçar os controles de segurança do PCI DSS?

Desenvolvemos um programa próprio para conformidade com o PCI DSS, mantido desde 2010. Nossa tarefa inicial era garantir o envolvimento de todas as áreas internas da empresa em uma operação integrada. Com base no conhecimento da importância do papel de cada uma das áreas diretamente envolvidas, demonstrando o impacto de sua atividade em uma cadeia e a entrega de resultados, conseguimos evoluir muito rapidamente, mantendo um programa muito bem estruturado e consistente.

Sua organização aproveitou o treinamento oferecido pelo PCI Council? Em caso afirmativo, como o treinamento beneficiou sua empresa?

Sim, e consideramos o treinamento fundamental. Hoje nós temos [Avaliadores de Segurança Interna \(ISA\)](#) e [Profissionais Certificados da Indústria de Cartões de Pagamento \(PCIP\)](#), além de participar também do treinamento informativo do [Qualified PIN Assessor \(QPA\)](#), que nos ajuda bastante nos processos da unidade de negócios do processador de adquirentes. Um benefício que isso proporciona é a agilidade para tomar decisões rápidas e consistentes em projetos críticos para nossos clientes, aderindo totalmente aos requisitos do PCI DSS e PCI PIN Security, para os quais fomos avaliados.

Como sua empresa gerencia efetivamente a implementação dos controles de segurança do PCI DSS?

Através de atuação efetiva da área de Segurança da Informação em novos projetos e do monitoramento de processos que já trazem a segurança integrada.

Um dos principais desafios é equilibrar a constante evolução e o lançamento de novas tecnologias com simplicidade, segurança e conformidade. Tudo precisa funcionar de forma transparente, independentemente da plataforma e tecnologia empregada. Sabemos que as novas tecnologias vêm para facilitar os processos, por isso buscamos sempre treinamento e desenvolvimento da equipe interna e apoio de especialistas para nos apoiar na implementação dessas novas tecnologias, para que trabalhem a nosso favor, aumentando a eficiência e também a segurança. Ter especialistas com uma visão holística para resolver problemas de segurança e conformidade faz toda a diferença em um ambiente crítico e regulamentado.

Como o PCI DSS ajudou a melhorar a postura de segurança da sua empresa?

O PCI DSS funciona hoje como nossa estrutura de segurança básica, sendo amplamente aplicado em nosso ambiente. Com cada novo projeto, mesmo que não esteja diretamente relacionado ao ambiente dentro do escopo, consideramos os requisitos em nossas recomendações internas para lidar com demandas. Desde que os requisitos do PCI DSS foram incorporados à nossa política de segurança, nosso grau de maturidade em segurança da informação aumentou consideravelmente, e temos certeza de que todos os pontos críticos foram devidamente tratados.

Como você e sua empresa planejam usar o conhecimento do PCI DSS?

Além de aplicar esse conhecimento ao objetivo principal de manter a conformidade com o PCI DSS, também planejamos usá-lo como uma estrutura padrão para aplicação em diferentes projetos, onde decisões de segurança são necessárias para processos semelhantes. Também planejamos treinar mais funcionários da empresa no PCI DSS, a fim de ter uma cultura de segurança da informação mais forte e consistente.

Brazil Regional Engagement Board

CSU Cardsystem S.A. é um membro ativo do [Conselho Consultivo Regional do Brasil](#), que representa as perspectivas das [Organizações Participantes](#) e dos constituintes do PCI SSC no Brasil, aconselhando e fornecendo feedback e orientação ao PCI SSC sobre desenvolvimento e adoção de padrões e programas no Brasil.