



ESTUDO DE CASO PCI Data Security Standard (PCI DSS)

A EMPRESA:



A FIS é uma provedora de soluções e serviços no mundo para a indústria financeira. A empresa oferece serviços de processamento de cartões para vários clientes na região da América Latina, serviços de call center para os emissores, back office e prevenção de fraudes.

Como provedor de serviços, como o PCI Data Security Standard (PCI DSS) ajuda sua empresa?

Embora já tenha uma forte postura de segurança, o PCI DSS ajuda a FIS promovendo uma abordagem disciplinada ao processo de conformidade. Ele cria uma boa visibilidade dos controles dentro da liderança sênior e fornece um vocabulário comum para os executivos.

Qual tem sido um desafio principal da sua empresa na implementação e manutenção dos controles do PCI DSS?

Um dos aspectos mais desafiadores para manter a conformidade com o PCI DSS é a constante evolução da tecnologia e suas aplicações. As empresas estão sempre pesquisando meios para equilibrar as necessidades de segurança, conformidade e negócios, e com o aumento da taxa de inovação e tecnologias inovadoras, é sempre um desafio acompanhar todos os controles e, ao mesmo tempo, apoiar a evolução da empresa.

E para uma empresa tão grande quanto a FIS, o maior desafio é coordenar várias avaliações simultâneas, ao mesmo tempo em que garante que a empresa não tenha vários modelos, processos e procedimentos distintos, respeitando a avaliação individual e as particularidades da região geográfica.

Como a empresa lidou com esse desafio?

Ao ter modelos comuns para orientar a preparação de evidências pelas várias unidades de negócios, uma abordagem programada para coordenar as várias avaliações e um conjunto forte de políticas implementadas em toda a organização ajuda a reduzir a entropia e cria um meio de medir a eficácia dessas definições entre os assessores atuais. Em relação ao desafio evolutivo, a única resposta que vejo é garantir que colocamos a conformidade com o PCI DSS como integrante de todos os processos que executamos na empresa.

Que resultados isso gerou?

Certificações sendo concluídas de forma consistente dentro do prazo esperado, uma abordagem consistente em várias unidades de negócios e transferência de conhecimento entre pares e abordagens de avaliação múltiplas.

Quais são as recomendações para empresas semelhantes quando se trata de implementar e manter o PCI DSS?

O programa para implementar e manter a conformidade com o PCI DSS deve ser permanente e com o devido empoderamento e supervisão. Um programa PCI DSS deve estar na agenda da liderança.

Conselho Consultivo Regional do Brasil

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