ESTUDO DE CASO

PCI Data Security Standard (PCI DSS)

Cielo é uma empresa de tecnologia e serviços para o segmento de pagamentos eletrônicos na América Latina. Oferecemos um portfólio de soluções para atender às necessidades de nossos mais de 1,5 milhão de comerciantes, de empreendedores individuais a grandes varejistas espalhados por todo o país. Temos uma estrutura que mantém os negócios em movimento, com tecnologia, logística e padrões de segurança.

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

Inicialmente a Cielo se apoiou nos programas de segurança das bandeiras para endereçar os controles do PCI DSS e, com a maturidade em segurança adquirida no escopo de meios de pagamentos, a Cielo passou a utilizar o PCI DSS para endereçar a construção de outras plataformas de suporte ao negócio. O PCI DSS também foi utilizado desde a logística de equipamentos até a gestão de clientes, auxiliando também na prevenção a fraudes.

Com o aprendizado em segurança propiciado pelo PCI DSS a Cielo passou a buscar apoio também nos frameworks recomendados pelo Council, como o NIST, para construção dos baselines de segurança e gestão de chaves criptográficas, além de utilizar o IT Score do Gartner para mensuração regular da maturidade em processos de segurança. Com base no resultado da análise do IT Score Gartner são definidos planos de ação para garantir a manutenção de nosso plano diretor de segurança.

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

Sim, a Cielo optou por qualificar os profissionais que trabalham na área de Segurança da Informação com o treinamento do Assessor de Segurança Interno (ISA) e também contou com a assistência dos parceiros Qualified Security Assessor (QSA) do PCI para treinamento em desenvolvimento seguro de aplicativos. Esses treinamentos permitiram que os funcionários de segurança e desenvolvimento da Cielo tivessem um conhecimento mais profundo do PCI DSS, o que resultou em discussões mais ricas e fundamentadas sobre os controles de segurança.

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

A conscientização de todos os colaboradores e o apoio da alta direção são fundamentais nesta jornada para garantir a manutenção dos controles de segurança. Com ajuda dos indicadores gerados pelo IT Score e pelas campanhas de segurança corporativa promovidas pela área de Segurança da Informação a Cielo estabelece planos que abrangem todas as camadas da companhia. Um dos maiores desafios quando iniciamos o processo foi lidar com sistemas legados que não tinham controles adequados para atender ao PCI DSS. A maneira de abordar esse problema era conscientizar todos os funcionários da empresa de que, para continuar processando as transações de maneira segura, era necessário envolver todos no mapeamento e na manutenção necessária dos sistemas. Outro desafio extremamente importante, que ainda está em andamento, refere-se à transformação digital para atender às novas demandas de negócios. A Cielo vem treinando profissionais, ouvindo seus clientes e se transformando digitalmente para atender às novas dinâmicas do mercado de pagamentos. Todo o trabalho realizado nos últimos anos culminou na conformidade com o PCI DSS pelo 10º ano consecutivo, demonstrando que o envolvimento da equipe da Cielo está funcionando.

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

O PCI DSS ajudou a melhorar o processo de segurança da Cielo porque nos permitiu identificar riscos em nossos ambientes e também em provedores de serviços que poderiam afetar a disponibilidade de nossos serviços. O PCI DSS nos permite criar indicadores para mostrar aos nossos executivos uma visão clara dos processos de negócios mais impactantes para a Cielo.

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

A Cielo levou as melhores práticas de segurança do PCI DSS para todos os projetos da empresa para tornar o ambiente mais robusto e resistente a falhas. Hoje, quando o tópico de segurança é abordado nas reuniões do projeto, o primeiro tópico a ser lembrado é o PCI DSS.

Como adquirente, como sua empresa oferece suporte aos comerciantes que adotam controles de segurança PCI DSS?

Um dos principais desafios para os comerciantes na adoção do PCI DSS foi o orçamento financeiro, devido ao alto investimento necessário para atualizar sistemas, substituir equipamentos e contratar pessoal qualificado. Para dar suporte aos clientes, a Cielo subsidiou serviços de segurança contratando QSAs do PCI para trabalhar com nossos comerciantes. Com esses serviços, foi possível avaliar vários comerciantes e também mostrar aos executivos os riscos aos quais as empresas estavam expostas e também os benefícios que o investimento em segurança pode trazer.

Brazil Regional Engagement Board

Cielo 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.