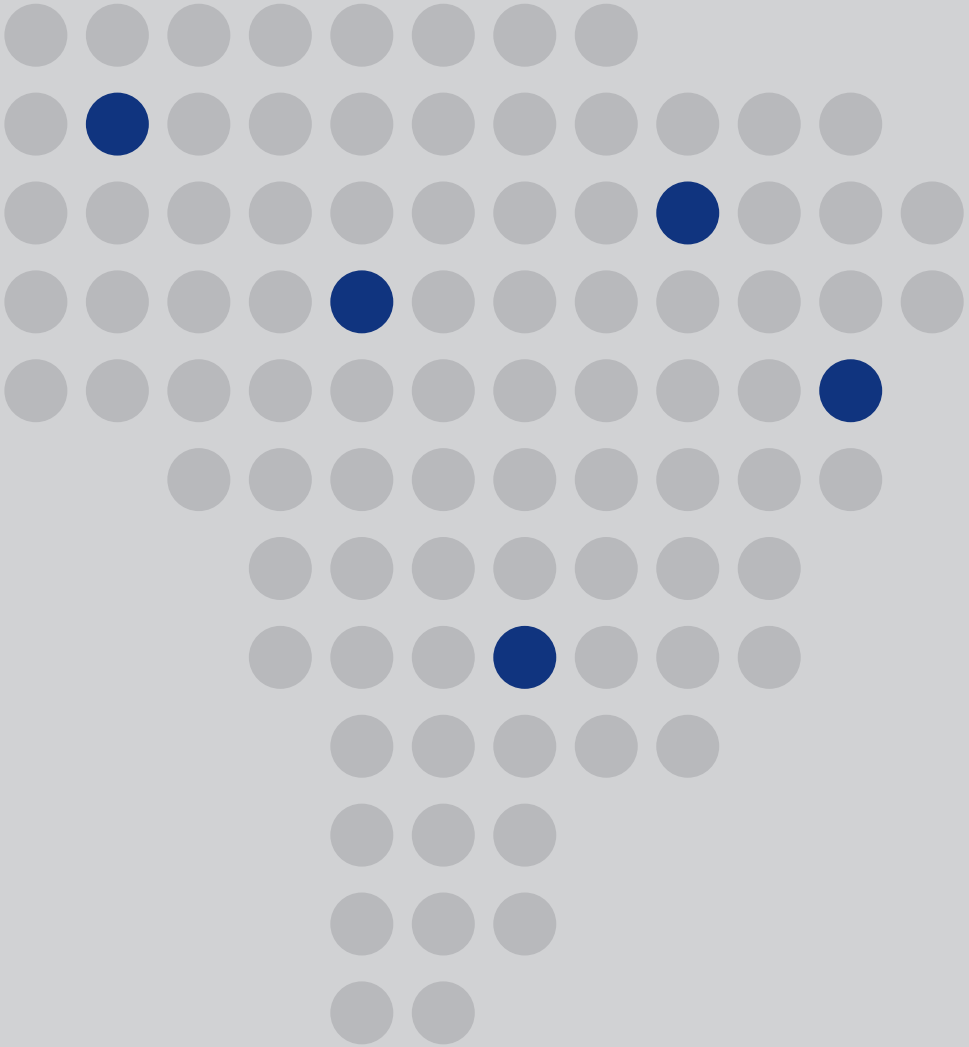
Roadmap de Segurança: Brasil 2019

VISA



Limitação de Responsabilidade

As informações, recomendações ou "melhores práticas" aqui contidas são fornecidas "COMO ESTÃO" e a título meramente informativo e, assim, não devem ser consideradas como uma assessoria de negócio, operacional, de marketing, financeira, jurídica, técnica, fiscal ou de qualquer outro tipo. Ao implementar qualquer nova estratégia ou prática, você deve consultar seu assessor jurídico para determinar as leis e regulamentos que podem ser aplicáveis à sua situação específica. Os custos reais, economias e benefícios resultantes de referidas recomendações, programas ou "melhores práticas" podem variar com base em suas necessidades específicas negociais e nos requisitos do programa. Pela sua natureza, as recomendações não são garantias de desempenho futuro ou resultados e estão sujeitas a riscos, incertezas e suposições que são difíceis de prever ou quantificar. Suposições foram feitas por nós à luz da nossa experiência e nossas percepções de tendências históricas, das condições atuais e dos desenvolvimentos futuros esperados e outros fatores que acreditamos sejam adequados sob a circunstancia. Recomendações estão sujeitas a riscos e incertezas, e os resultados e tendências reais e futuros podem diferir materialmente das suposições ou recomendações.

A Visa não é responsável pelo uso que você faça da informação aqui contida (incluindo erros, omissões, imprecisões ou faltas de oportunidades de qualquer tipo) ou por quaisquer suposições ou conclusões que você possa tirar do seu uso. A Visa não oferece nenhuma garantia, expressa ou implícita e renuncia explicitamente as garantias de comercialização e adequação a uma finalidade específica, a toda e qualquer garantia de não violação de direitos de propriedade intelectual de qualquer terceiro, qualquer garantia de que a informação irá atender aos requisitos de um cliente ou qualquer garantia de que a informação é atualizada e será livre de erros. Na extensão permitida pela lei aplicável, a Visa não será responsável perante um cliente ou qualquer terceiro por quaisquer danos ou prejuízos previstos em lei, incluindo, sem limitação, danos especiais, emergentes, incidentais ou punitivos, nem quaisquer danos por lucros cessantes, interrupção de negócios, perda de informações comerciais ou outras perdas monetárias, mesmo se tiver sido notificado da possibilidade de tais danos.

Sumário Executivo

Na Visa, acreditamos que a segurança deve avançar tão rápido quanto a inovação

A Visa é líder em segurança de pagamentos por mais de 60 anos, com inovações que acompanharam os avanços tecnológicos e a evolução das fraudes dentro do ecossistema. Isso nos ajudou a manter a fraude em níveis historicamente muito baixos.

Adotamos o princípio da inovação responsável. Isso quer dizer que qualquer nova capacidade desenvolvida pela Visa precisa ser segura. É nossa responsabilidade equilibrar segurança com experiências de pagamento cada vez melhores - entendemos que uma não pode existir sem a outra. Para isso a Visa continua investindo para aumentar a segurança em todo o ecossistema de pagamento e, ao mesmo tempo, melhorar a experiência do consumidor ao pagar.

A Visa vem trabalhando com parceiros e padrões da indústria na evolução da segurança para o ecossistema de pagamentos do Brasil, focando fortemente na tecnologia de Chip (EMV) e promovendo a conformidade com o PCI DSS (Padrão de Segurança de Dados da Indústria de Cartões de Pagamento).

Juntos, tornamos a tecnologia do Chip EMV quase onipresente, introduzimos a utilização do PIN como um padrão do mercado e colaboramos em muitas outras iniciativas para melhorar a segurança da indústria como um todo.

Muitas dessas soluções buscam proteger os pagamentos usando tecnologias específicas para o ambiente, como a tecnologia de Chip no ambiente presencial ou a autenticação por senha no e-commerce. Atualmente as coisas não são mais só brancas ou pretas e existem nuances que a segurança precisa considerar.

As características de um pagamento realizado com a presença do portador e um pagamento realizado remotamente estão cada vez mais próximas. As compras via aplicativo (in-app) são um exemplo de pagamento remoto acontecendo em um ambiente presencial. Consequentemente, os pagamentos serão cada vez mais baseados na conta digital – e não no cartão físico. É por isso que, cada vez mais, usaremos o termo 'portador de conta', em vez de ´portador de cartão´. Essa aproximação das características cria um novo paradigma de como devemos proteger os pagamentos, sempre baseado no princípio da Visa de usar múltiplas camadas de segurança, desenhadas para atuar em conjunto e garantir pagamentos confiáveis, seguros e convenientes. Isso é fundamental para mantermos e fortalecermos a confiança do consumidor em todas as transações.

O Roadmap de Segurança da Visa considera quatro pilares estratégicos:

Desvalorizar os dados eliminando dados sensíveis (e.g. números de cartões) do ecossistema impossibilitando o uso caso sejam roubados.

Proteger os dados implantando medidas de segurança para proteger tanto dados pessoais como informações de cartões e contas digitais.

Utilizar os dados identificando potenciais fraudes antes que elas ocorram e aprovando transações legítimas com mais confiança.

Empoderar todos os envolvidos como portadores de contas, prestadores de serviços e estabelecimentos comerciais, tornando-os aptos a contribuir com a segurança dos pagamentos.

O Roadmap

O Roadmap da Visa para o futuro da segurança: Brasil

Objetivo: Aumentar a segurança em todo o ecossistema de pagamento. Adotamos o princípio da inovação responsável: otimizar o equilíbrio entre risco e inovação.

Desvalorizar Dados

Proteger Dados

Utilizar Dados

Empoderar Todos

Existente	2020	2021	2022 +
Segurança Trans. Cartão Presente 99% POS: 100%[1] Chip, emissor Chip Contacless, emissor: 0.9% POS: 81%[2]	**Segurança Trans. Cartão Presente** Acelerar expansão Contactless focando em transporte e uso diário/corriqueiro	**Segurança Trans. Cartão Presente** Expandir pagamentos Contactless a novos segmentos	**Segurança Trans. Cartão Presente** Mercado 100% Chip Contactless e incorporando autenticação por biometria
Tokens/Secure Remote Commerce Introdução de novos padrões e primeiras implementações (Card on File – CoF / Tokens carteiras)	**Tokenizar Cartões em Arquivo (CoF)** Acelerar adoção de tokenização em comércios CoF de grande porte	**Tokenizar Cartões em Arquivo (CoF)** Expandir a utilização de cartões tokenizados para todos os comércios CoF no mercado	**Tokenizar Cartões em Arquivo (CoF)** Adoção massiva de Tokens, eliminando números de cartão em comércios CoF
Segurança do Ecossistema Promover adoção de tecnologias mais robustas elevando o nível de segurança do ecossistema	**Secure Remote Commerce (SRC)** Alinhamento de mercado para criar plano de implantação	**Secure Remote Commerce (SRC)** Viabilizar primeiras implementações seguindo alinhamento de mercado	**Secure Remote Commerce (SRC)** Expandir adoção do SRC conforme alinhamento de mercado
Padrões de Segurança de Dados PCI Alto nível de cumprimento	**Padrões de Segurança de Dados PCI** Cumprir padrões PCI atualizados	**Padrões de Segurança de Dados PCI** Cumprir padrões PCI atualizados	**Padrões de Segurança de Dados PCI** Cumprir padrões PCI atualizados
Ferramentas de Prevenção a Fraude Todos os emissores devem utilizar Ferramentas baseadas em score de riscos gerado em tempo real	**Ferramentas de Prevenção a Fraude** Todos os emissores devem utilizar Ferramentas baseadas em score de riscos gerado em tempo real	**Ferramentas de Prevenção a Fraude** Todos os emissores devem incorporar scores 3DS/token para autenticação de comércios e usuários	**Ferramentas de Prevenção a Fraude** Emissores prevenindo fraudes em colaboração com comércios usando ferramentas conectadas em tempo real
3D Secure 2.0 Expandir adoção de 3DS2 em comércios e emissores relevantes	**3D Secure 2.0** Expandir adoção de 3DS2 em comércios e emissores relevantes	**3D Secure 2.0** Primeiras implementações do conceito de autenticação baseada em riscos suportadas pelos dados do protocolo	**3D Secure 2.0** Utilizar com eficiência os dados do protocolo para garantir mínima intervenção do usuário
Alertas de Transações Todos os emissores oferecendo serviço de alertas	**Otimizar Recusas de Transações** Promover utilização correta e maior transparência focando em melhor experiência para o comércio e portador	**Otimizar Recusas de Transações** Promover utilização correta e maior transparência focando em melhor experiência para o comércio e portador	**Otimizar Recusas de Transações** Promover utilização correta e maior transparência focando em melhor experiência para o comércio e portador
	Alertas + Controle de Transações Agregar aos serviços de Alertas de Transações a capacidade do portador customizar características de uso de seu cartão	**Alerta + Controle de Transações** Promover adoção e utilização por parte dos portadores de conta	

***1,2** Baseado em Cartões e POS habilitados no mercado, Jun'19*
***3 B**aseado no PV Emissor habilitados no mercado e PV comercio LAC*

Regras Visa

Desvalorizar Dados

Segurança em Transações com Cartão Presente

Onde estamos hoje

A introdução da tecnologia de Chip (EMV) aprimorou a segurança e abriu caminho para inovações como pagamentos por aproximação e via dispositivos móveis como smartphones. Os cartões com Chip geram um código exclusivo e de uso único a cada vez que são usados em um terminal compatível com a tecnologia de Chip. Por ser quase impossível de ser duplicada, essa funcionalidade previne a ocorrência de fraudes com cartões falsificados.

Por conta disso a Visa introduziu em suas regras a obrigação de que novos cartões emitidos e terminais POS instalados no mercado tenham a capacidade Chip e Chip sem contato (Contactless).

Para onde estamos indo

Estamos trabalhando com nossos emissores e estabelecimentos comerciais para que 100% dos terminais, caixas eletrônicos e cartões emitidos no mercado Brasileiro sejam compatíveis com a tecnologia Chip EMV.

Também estamos trabalhando na expansão dos pagamentos Chip sem contato para melhorar a experiência de pagamento, proporcionando maior conveniência e velocidade com a mesma segurança do Chip. As plataformas de pagamento sem contato permitem pagamentos gerados a partir de dispositivos móveis, incorporando uma ampla variedade de novos elementos de segurança por meio de dados biométricos (por exemplo: voz, reconhecimento facial ou impressão digital).

As plataformas de pagamento sem contato permitirão a expansão de pagamentos com cartões em novas categorias de estabelecimentos comerciais, entre elas transportes e compras diárias ou corriqueiras de baixo valor. Elas vêm com foco em uma experiência de pagamento centrada no consumidor que leva cada vez mais seu cartão ou dispositivo móvel consigo.

- **2020:** Acelerar expansão Contactless focando em transporte e uso diário/corriqueiro
- **2021:** Expandir os pagamentos sem contato para novos segmentos
- **2022 em diante:** Alcance 100% de aceitação do Chip EMV com / sem contato incorporando novos elementos de segurança biométrica

VISA

Desvalorizar Dados

Tokenização

Onde estamos hoje

Em 2013, a Visa ajudou a liderar um esforço colaborativo da indústria global em prol da tokenização dos pagamentos e foi fundamental para o desenvolvimento das Especificações de Tokenização de Pagamentos da EMV®.

A tokenização é uma iniciativa da indústria de pagamento que adiciona mais uma camada de segurança aos pagamentos móveis e digitais. Ela remove dados sensíveis do ecossistema do estabelecimento comercial e evita fraudes que envolvem diferentes canais, sem adicionar atrito à experiência de compra.

O objetivo de segurança do processo de tokenização é substituir certas informações dos portadores de contas – como os números e as datas de validade dos cartões – por um identificador digital exclusivo (um "token"). O token é exclusivo para um dispositivo, provedor de carteira digital ou caso de uso – por exemplo, estabelecimentos comerciais CoF (sigla em inglês para credencial em arquivo, credential-on-file).

Para onde estamos indo

A Visa trouxe os serviços de token para o mercado Brasileiro para apoiar a adoção dos pagamentos móveis e gerar segurança e simplicidade para o mercado promover inovações como CoF, tecnologias wearables e também a internet das coisas (IoT).

A tokenização é parte de uma estratégia de longo prazo da Visa para proteger os pagamentos digitais. A meta é garantir que todos os dados de cartões mantidos fora das instituições financeiras estejam tokenizados até 2022.

- **2020:** Acelerar adoção de tokenização em estabelecimentos comerciais CoF de grande porte
- **2021:** Expandir a utilização de Cartões tokenizados para todos os estabelecimentos comerciais CoF no mercado
- **2022 em diante:** Adoção massiva de Tokens, eliminando números de cartão em estabelecimentos comerciais CoF

CoF ou Credencial em Arquivo

O crescimento do comércio digital e a emergência de novos modelos de negócios geraram um aumento de transações nas quais as credenciais de pagamento dos portadores de contas (ex.: número de cartão ou token) são mantidas em bases de dados de um comércio, provedor de carteira digital ou outro prestador de serviços para serem usadas em futuras transações.

Desvalorizar Dados

Secure Remote Commerce (SRC)

Onde estamos hoje

Em 2018, a EMVCo anunciou as especificações do EMV® Secure Remote Commerce (SRC) para melhorar de forma segura a experiência de portadores de conta com transações não presenciais. Essas especificações criaram as fundações que permitirão o processamento de transações de comércio eletrônico de maneira simples e consistente através de múltiplos canais e dispositivos.

Para onde estamos indo

Os Estabelecimentos Comerciais criaram soluções fragmentadas e sem padrões para resolver os desafios relacionados à segurança das credenciais de pagamento (e.g., dados sensíveis e números de cartões) e também diferentes formas para verificação dos portadores de cartão. A experiência do portador de conta se tornou inconsistente e confusa.
Para resolver esses problemas, a indústria global colaborou com a EMVCo criando um padrão seguro e eficiente para estabelecimentos comerciais remotos cobrindo a captura, transmissão e armazenamento destas credenciais de pagamento.

As especificações EMV SRC permitirão:

- Um padrão de experiência de pagamento consistente para todas as marcas participantes;
- Padronização para processamento e integração de várias redes de pagamento, substituindo dados confidenciais de cartão por tokens; e
- Segurança integrada e com interoperabilidade total com o 3D-Secure para autenticar e verificar o portador da conta no momento da compra.

Como parte das especificações do SRC, a funcionalidade do "Cloud Token" passa a ser incorporada aos serviços de token. Essa nova funcionalidade permite melhorias significativas que incluem: Vinculo (link) de dispositivo-token, autenticação do consumidor por meio de vários fatores, gerenciamento de ciclo de vida para credenciais de pagamento e utilização de dispositivos confiáveis.

O método de verificação através do dispositivo consumidor (CDCVM) também vem para suportar estas inovações. O CDCVM captura o método de verificação do portador de cartão (CVM) em um dispositivo de pagamento móvel (e.g. smartphone ou tablet) e, assim, o cliente pode mostrar de forma rápida, simples e segura que ele é o usuário genuíno.

Para formas de autenticação, a Visa não se inclina nem promove ativamente um único tipo de biometria. Ela vem trabalhando com associações do setor para certificar múltiplas formas e produtos de autenticação biométrica objetivando facilitar a adoção por seus membros.

- **2020:** Alinhamento de mercado para criar plano de implantação
- **2021:** Viabilizar primeiras implementações seguindo alinhamento de mercado
- **2022 em diante:** Expandir adoção do SRC conforme alinhamento de mercado

EMVCo

A EMVCo existe para facilitar a interoperabilidade e a aceitação de transações com pagamentos seguros em todo o mundo. O trabalho da EMVCo é monitorado por suas seis organizações membros, incluindo a Visa, e é apoiado por dezenas de emissores, empresas, processadores, fornecedores e outros participantes do setor.

Programa de Comércio Digital Visa

A Visa lançou o programa de comércio digital (Visa Digital Commerce Program - VDCP) para trazer ao ambiente online os benefícios de padrões comuns de aceitação em pontos de venda físicos. Com base na estrutura técnica do EMVCo Secure Remote Commerce (Comércio remoto seguro - SRC), o programa VDCP permitirá transações comerciais digitais consistentes e seguras a partir de qualquer dispositivo e aprimorará a experiência do cliente. O VDCP prevê total interoperabilidade com as especificações de tokenização e 3-D Secure também parte deste roadmap e, juntas, elas formam uma base para a estratégia de desvalorização de dados da Visa para todos os pagamentos via aplicativo (in-app) ou no navegador.

Proteger Dados

Segurança do Ecossistema

Onde estamos hoje

Por mais de uma década, o mercado Brasileiro tem seguido em direção à tecnologia de Chip com contato e sem contato. Este movimento, muito promovido pela Visa, resultou em taxas de aprovação mais elevadas e índices mais baixos de fraude que, por sua vez, aprimoraram a experiência do portador de cartão e a confiança do consumidor. Mais de 99 por cento dos pagamentos com presença do portador efetuados no Brasil são de transações originadas em cartões Chip lidos em terminais de ponto de venda (POS) que suportam a tecnologia Chip.

Baseada nos resultados, a Visa atualizou suas regras para motivar Emissores e Credenciadores a concluírem a atualização de seus portfólios de cartões e terminais de ponto de venda (POS) para tecnologia Chip.

Para onde estamos indo

A partir de Abril de 2019 a Visa passou a motivar emissores Brasileiros a reduzir a aprovação de transações com cartões sem Chip (e.g. tarja magnética) feitas em estabelecimentos comerciais também Brasileiros. Passou também a motivar os emissores a não aprovar transações que possuam dados referentes a segurança do Chip (criptogramas) ausentes ou inválidos.

Da mesma forma, a partir de Abril de 2019, credenciadores passaram a ser motivados a evitar a captura de transações sem Chip (e.g. tarja magnética, transações digitadas) em terminais de ponto de venda e caixas eletrônicos (ATM).

Transações que atendam os critérios definidos acima são, por definição, percebidas e tratadas como menos seguras e diante da disponibilidade de terminais de ponto de venda (POS) suportando a tecnologia Chip, a Visa considera que esta iniciativa promoverá a adoção de padrões mais seguros em curto prazo.

- **2019 em diante:** Promover adoção de tecnologias mais robustas elevando o nível de segurança do ecossistema

Proteger Dados

Padrões de Segurança de Dados PCI

Onde estamos hoje

A conformidade com o PCI DSS é a base dos programas de Segurança de Dados e Conformidade da Visa e fundamental para impedir o comprometimento de dados sensíveis dos portadores de contas. O PCI-DSS estabelece requisitos técnicos e operacionais que ajudam as organizações (estabelecimentos comerciais, instituições financeiras, processadores de pagamento, prestadores de serviços e provedores de tecnologia) a manter defesas de Segurança da Informação prontas para proteger os dados dos portadores de contas de ataques realizados com intento de roubo.

A Visa estabeleceu requisitos específicos que definem os critérios que as entidades participantes do seu arranjo de pagamentos devem seguir para demonstrar a conformidade com os padrões PCI.

Para onde estamos indo

O padrão PCI DSS é atualizado com frequência introduzindo novos requisitos e controles para mitigar novas ameaças cujo alvo são as informações de pagamento.

As empresas que armazenam, processam ou transmitem informações de portadores de contas devem estar em conformidade com a versão mais recente publicada pelo PCI-DSS para prevenir, detectar e responder a ataques cibernéticos que possam resultar em comprometimento e obtenção indevida de dados.

- **2020 em diante:** Promover o cumprimento das normas atualizadas do PCI

Padrões de segurança de dados do PCI

O PCI Security Standards Council é uma organização global criada com o objetivo de desenvolver, melhorar, disseminar e educar sobre padrões de segurança para meios de pagamento. Foi criado em setembro de 2006 e é composto pelas principais organizações de meios de pagamento. Todas essas entidades concordaram em incorporar os Padrões de Segurança de Dados (PCI-DSS) como parte de seus requisitos técnicos para seus programas de conformidade de segurança de dados.

Utilizar Dados

Ferramentas de Prevenção a Fraude

Onde estamos hoje

A Visa exige, desde julho de 2018, que todos os emissores da região da América Latina usem ferramentas de prevenção de fraudes com base em pontuações (scores) de risco gerados em tempo real.

Para onde estamos indo

O gerenciamento de riscos é uma tarefa fundamental para manter a confiança no sistema de pagamentos. A Visa espera que os emissores mantenham um processo dinâmico e eficiente que lhes permita identificar transações fraudulentas em tempo real e tomar ações para detê-las.

Os emissores devem ser capazes de incorporar novos elementos de segurança em suas ferramentas de prevenção de fraudes, tais como: transações não financeiras, resultados de autenticação com token e 3DS, biometria, etc.

- **2020:** Todos os emissores devem utilizar Ferramentas baseadas em score de riscos gerado em tempo real
- **2021:** Todos os emissores devem incorporar scores 3DS/token para autenticação de estabelecimentos comerciais e usuários
- **2022 em diante:** Emissores prevenindo fraudes em colaboração com estabelecimentos comerciais usando ferramentas conectadas em tempo real

Ferramentas adicionais - Geolocalização

Transações suspeitas costumam ser recusadas para prevenir fraudes. Porém, nem todas as transações consideradas suspeitas são fraudulentas. Para prevenir fraudes e evitar a recusa desnecessária de transações, o serviço Visa Mobile Location Confirmation fornece, em tempo quase real[1], as informações de geolocalização dos portadores de contas registrados no serviço. Isso torna possível ao emissor determinar se o dispositivo do portador da conta está nas proximidades do estabelecimento comercial. Com esta tecnologia, os emissores conseguem aprovar transações legítimas com mais confiança, ajudando a oferecer uma melhor experiência ao consumidor e a evitar custos operacionais associados a transações incorretamente recusadas e a ligações para aviso de viagem. As APIs Mobile Location Confirmation estão disponíveis no Visa Developer (https://developer.visa.com/).

1 o tempo que o alerta leva para chegar dependerá do serviço sem fio e da cobertura dentro da área.

VISA

Proteger Dados

3D Secure 2.0

Onde estamos hoje

O protocolo 3-Domain Secure (3DS) permite que os consumidores se autentiquem direto com o emissor no momento em que fazem suas compras online. O objetivo do 3DS é melhorar a segurança, evitando o uso não autorizado de cartões Visa no ambiente online.

A adoção do 3DS no mercado Brasileiro tem sido relativamente baixa devido ao atrito na experiência de compra online. O lançamento da nova versão do protocolo veio para solucionar este atrito e é um bom exemplo do que a Visa considera Inovação Responsável: melhorar a segurança tornando o consumidor parte do processo enquanto melhoramos a experiência de pagamento.

Para onde estamos indo

Para alcançar esse objetivo, a EMVCo publicou uma nova versão para as especificações 3DS. A nova versão permite que os portadores de conta autentiquem sua identidade com mais facilidade, em tempo real, e promovendo uma maior troca de dados entre estabelecimentos comerciais e emissores de formas mais convenientes deixando o processo transparente para o consumidor.

- **2020:** Expandir adoção de 3DS2 em estabelecimentos comerciais e emissores relevantes
- **2021:** Primeiras implementações do conceito de autenticação baseada em riscos suportadas pelos dados do protocolo
- **2022 em diante:** Utilizar com eficiência os dados para garantir mínima intervenção do usuário

Proteger Dados

Otimizar Recusas de Transações

Onde estamos hoje

O processamento de autorizações exige um delicado equilíbrio entre todos os participantes. Garantir o fluxo adequado de informações é essencial para gerar um comportamento ótimo. Uma análise minuciosa da abordagem de autorização destacou o fato de que, atualmente, os códigos de recusa oferecem valor limitado ao ecossistema pois, por padrão, são utilizadas razões vagas para um grande número de recusas ou são utilizadas definições que oferecem valor mínimo para credenciadores e estabelecimentos comerciais tentarem converter uma venda após uma recusa.

Essa prática cria um alto volume de novas tentativas mal focadas por parte dos estabelecimentos comerciais, já que eles não conseguem diferenciar facilmente uma recusa de baixo risco (por exemplo, falta de fundos ou alguma pequena falha no processamento) de uma recusa de alto risco (por exemplo, cartão bloqueado ou envio de dados incorretos), o que resulta em custos mais altos, processos de detecção ineficientes e consumidores confusos.

Para onde estamos indo

A Visa reposicionará os códigos de resposta de recusa para torná-los mais úteis, minimizando, ao mesmo tempo, os comportamentos danosos ou que geram custos. Os códigos de recusa existentes serão agrupados em categorias nas quais os emissores deverão operar quando lidam com solicitações de autorização, o que também exigirá alterações no processamento de códigos de resposta.

A partir de Abril de 2020 a Visa tornará vigente um novo conjunto de regras para motivar a utilização correta, a consistência nos dados e também uma maior transparência nas mensagens de forma a permitir que todo o ecossistema identifique claramente a razão das recusas pelos emissores. Desta forma, credenciadores e estabelecimentos comerciais podem, com base nestas respostas, executar estratégias mais eficientes para oferecer uma melhor experiência de compra para os portadores de contas.

- **2020 em diante:** Promover utilização correta e maior transparência focando em melhor experiência para o estabelecimento comercial e portador

Empoderar a Todos

Alertas e Controles de Transações

Onde estamos hoje

A Visa exige, desde outubro de 2017, que todos os emissores de cartões de crédito, débito ou pré-pagos recarregáveis na região da América Latina ofereçam uma opção para clientes Visa se registrarem em um serviço de alertas.

Para onde estamos indo

Os portadores de contas esperam cada vez mais controlar todos os aspectos diários de suas vidas e isto inclui compras, entretenimento, comunicações, notícias, etc. Eles esperam o mesmo nível de controle para gerenciar seus produtos bancários como também controlar a maneira como pagam.

Os dispositivos móveis oferecem uma excelente oportunidade para capacitar os consumidores por meio de aplicativos. Eles permitem que o portador gerencie de maneira conveniente suas contas e também características e funcionalidades de seus cartões, melhorando a satisfação do cliente e ao mesmo tempo lhe dando um papel ativo no gerenciamento de riscos.

- **2020:** Agregar aos serviços de Alertas de Transações a capacidade do portador customizar características de uso para seu cartão
- **2021 em diante:** Promover adoção e utilização por parte dos portadores de conta

Controle de Transações Visa (VTC)

A crescente preferência do consumidor por serviços de autoatendimento e controle sobre sua forma de pagar levou à criação do Visa Transaction Controls, onde os portadores de contas podem definir limites de gastos, restringir pagamentos em certos canais, proibir transações internacionais ou mesmo suspender temporariamente o cartão em caso de extravio ou perda/roubo. O serviço Transaction Controls aumenta a segurança e ajuda o consumidor a gerenciar melhor seus gastos; ao mesmo tempo, conquista sua confiança e preferência no uso do cartão. O serviço é disponibilizado aos consumidores por meio de seus emissores.

Os emissores Visa também podem ajudar o consumidor a controlar e a gerenciar melhor suas despesas, por meio do serviço Visa Transaction Alerts. Ele permite que os portadores de contas enxerguem as transações realizadas com seus cartões Visa registrados quase que em tempo real[1]. Os portadores podem selecionar os tipos de alerta e os gastos que dispararão as notificações personalizadas, que lhes são enviadas por e-mail e/ou SMS. As APIs Transaction Controls e Transaction Alerts da Visa estão disponíveis no Visa Developer.

1 O tempo para recebimento do alerta de transação depende do serviço de telefonia móvel e da cobertura na área.

VISA

Iniciativas

A Visa colabora com seus membros (emissores, credenciadores, agentes), stakeholders da indústria, reguladores, forças da lei e consumidores para manter o ecossistema de pagamentos seguro e prevenir fraudes. A abordagem de segurança de múltiplas camadas que implantamos manteve os níveis de fraude baixos, mesmo com o crescimento expressivo no volume de pagamentos eletrônicos. Entretanto, todos têm a responsabilidade de continuar protegendo o ecossistema.

Veja como você pode ajudar:

Consumidores

- Use as funcionalidades de segurança de seu emissor, como alertas e controles de transação e geolocalização. Leia todas as dicas de segurança disponíveis
- Monitore suas contas e cartões com frequência e denuncie atividades suspeitas o quanto antes via os canais oficiais disponibilizados por seu emissor
- Não responda a e-mails, mensagens de texto ou ligações supostamente do seu emissor ou da Visa que solicitem informações pessoais. Comunique qualquer atividade suspeita à seu emissor

Prestadores de serviços

- Não deixe de validar a conformidade com o PCI DSS em todos os ambientes de armazenamento, processamento ou transmissão de dados de cartões Visa
- Trabalhe com os emissores e credenciadores para fazer seu registro de Agente Externo (Third Party Agent – TPA) com a Visa. Os prestadores de serviços que estão em conformidade são incluídos no Registro Global de Prestadores de Serviços da Visa no www.visa.com/onthelist

Estabelecimentos Comerciais

- Certifique-se de que 100% dos seus terminais aceitem o Chip EMV com / sem contato
- Fale com seus prestadores (e.g. gateways) sobre a tokenização
- Gerencie fraudes antes de enviar as transações para autorização através de soluções baseadas em risco, incluindo o protocolo 3DS 2.0 se você for um e-commerce
- Cumpra os requisitos das versões vigentes do PCI DSS e os demais requisitos de segurança aplicáveis
- Use empresas registradas pela Visa para aceitar pagamentos e fazer o gerenciamento de fraude
- Mantenha-se atualizado sobre boas práticas de segurança para se proteger de fraudes

Credenciador

- Forneça orientações e informações a respeito de melhores práticas de segurança nos pagamentos aos seus estabelecimentos comerciais
- Habilite a tokenização e o processamento de CoF
- Trabalhe com os seus estabelecimentos comerciais para eliminar dados sensíveis e adotar as transações tokenizadas sempre que possível
- Registre todos os Prestadores de Serviços que tiverem acesso a dados de cartões Visa em seu nome ou em nome dos estabelecimentos comerciais

Emissor

- Proteja os dados do portador de conta com tokenização e emitindo 100% dos cartões com Chip EMV
- Forneça orientações e informações a respeito de melhores práticas de segurança nos pagamentos aos portadores de contas
- Forneça aplicativos com funcionalidades de segurança opcionais (ex.: alertas por push, controles de transação, geolocalização)
- Habilite os portadores de contas na versão mais recente do 3DS e utilize dados dinâmicos na autenticação
- Observe os requisitos mínimos de gestão de riscos para toda e qualquer iniciativa, produto ou serviço que proponha inovação nos pagamentos

Forças da lei

- Trabalhe com a indústria no combate à fraude
- Ajude a divulgar as novas tendências de fraude na indústria de pagamento

Notas


VISA