**Nuevas Normativas de Seguridad de VISA para Comercios Electrónicos**

Análisis y Directrices para la Implementación de Medidas de Protección en Transacciones Digitales

27/04/2025

# 1. Executive Summary

* Ejecutivo\*\*

El informe detalla las nuevas reglas de seguridad de VISA para comercios electrónicos, que entrarán en vigor el 15 de abril de 2025, tras su publicación el 29 de enero de 2025. Se introducen dos extensiones de mensaje globales: la Visa Additional Data Extension (VAD), que mejorará la seguridad de las transacciones electrónicas mediante el intercambio de datos adicionales, y la Visa Program Data Extension (VPDE), que ayudará a verificar el cumplimiento de los programas de autenticación de VISA. Aunque compartir datos será opcional, el Número de Orden de Compra será obligatorio para participar en el programa CE3.0. Además, se refuerzan los requisitos de seguridad de la información, exigiendo a los miembros de VISA mantener registros seguros y cumplir con los estándares PCI DSS. Finalmente, se implementarán recargos por incumplimiento escalonados para los comercios de Nivel 3, con el objetivo de mejorar la seguridad ante eventos de compromiso.

# 2. Alcance

## Alcance del Informe

El presente informe tiene como propósito proporcionar un análisis exhaustivo de las nuevas reglas de seguridad de VISA para comercios electrónicos, con un enfoque en las especificaciones y directrices que se implementarán a partir de 2025. Este documento está diseñado para ser una herramienta informativa para comerciantes, adquirentes, proveedores de servicios de pago y otros interesados en el ecosistema de comercio electrónico que buscan entender y adaptarse a las nuevas normativas de seguridad.

## Límites del Informe

1. \*\*Temporalidad\*\*: El informe se basa en la documentación y las regulaciones publicadas hasta la fecha de enero de 2025, y no incluye cambios o actualizaciones que puedan surgir después de esta fecha.

2. \*\*Enfoque en VISA\*\*: Aunque se mencionan aspectos generales de seguridad en el comercio electrónico, el informe se centra exclusivamente en las nuevas reglas y especificaciones de VISA, sin abordar normativas de otras entidades o redes de pago.

3. \*\*Aspectos Técnicos\*\*: Se proporcionará un resumen de las especificaciones técnicas relevantes, pero no se incluirán detalles técnicos exhaustivos ni guías de implementación específicas para sistemas de pago o plataformas de comercio electrónico.

4. \*\*Contexto Legal y Normativo\*\*: El informe no pretende ofrecer asesoría legal o cumplimiento normativo más allá de las directrices de VISA. Se recomienda a los comerciantes y adquirentes consultar con expertos legales para asegurar el cumplimiento de todas las regulaciones aplicables.

5. \*\*Perspectivas de Mercado\*\*: Este informe no incluye análisis de mercado o estudios de impacto económico relacionados con la implementación de las nuevas reglas de seguridad de VISA.

En resumen, el informe se limita a proporcionar una visión clara y concisa de las nuevas reglas de seguridad de VISA, facilitando a los interesados la comprensión de los cambios y su relevancia en el contexto del comercio electrónico.

# 3. Análisis Regulatorio

## Análisis Regulatorio de las Nuevas Reglas de Seguridad de VISA para Comercios Electrónicos

## 1. Principales Requisitos Normativos Identificados

## 1.1 Nuevas Extensiones de Mensaje Globales

* \*\*Visa Additional Data Extension (VAD)\*\*: Permite el envío y recepción de datos adicionales para mejorar la seguridad de las transacciones electrónicas.
* \*\*Visa Program Data Extension (VPDE)\*\*: Facilita la verificación del cumplimiento de los programas de autenticación de VISA.

## 1.2 Requisitos de Seguridad de la Información

* Mantenimiento seguro de registros de información de cuentas y transacciones.
* Cumplimiento con los estándares del \*\*Payment Card Industry Data Security Standard (PCI DSS)\*\*.

## 1.3 Actualización del Documento 'What To Do If Compromised'

* Implementación de recargos por incumplimiento escalonados para comercios de \*\*Nivel 3\*\*.

## 1.4 Cambios en los Requisitos de Campos de Datos

* Inclusión obligatoria del campo de \*\*dirección del destinatario\*\* en transacciones AFT transfronterizas a partir del \*\*11 de julio de 2025\*\*.

## 1.5 Control de Sanciones

* Revisión de programas de control de sanciones para asegurar que no se proporcionen productos de VISA a tarjetahabientes o comercios bajo sanciones.

## 2. Obligaciones para las Entidades Reguladas

## 2.1 Comercios y Adquirentes

* \*\*Implementación de Nuevas Extensiones\*\*: Los comercios deben estar preparados para enviar y recibir datos adicionales a partir del \*\*15 de abril de 2025\*\*.
* \*\*Cumplimiento con PCI DSS\*\*: Asegurar que todos los empleados con acceso a información de cuentas cumplan con los estándares de seguridad.

## 2.2 Miembros de VISA

* \*\*Mantenimiento de Registros\*\*: Asegurar que la información de cuentas y transacciones esté protegida y accesible solo para personal autorizado.
* \*\*Revisión de Programas de Sanciones\*\*: Actualizar y revisar los programas de control de sanciones para evitar el incumplimiento.

## 3. Procesos de Cumplimiento Necesarios

## 3.1 Preparación para Nuevas Extensiones de Mensaje

* \*\*Capacitación\*\*: Capacitar al personal sobre las nuevas especificaciones de VAD y VPDE.
* \*\*Actualización de Sistemas\*\*: Modificar los sistemas de procesamiento de pagos para incluir las nuevas extensiones de mensaje.

## 3.2 Implementación de Seguridad de la Información

* \*\*Auditorías Internas\*\*: Realizar auditorías regulares para verificar el cumplimiento con PCI DSS.
* \*\*Control de Acceso\*\*: Establecer controles de acceso estrictos para la información sensible.

## 3.3 Gestión de Recargos por Incumplimiento

* \*\*Evaluación de Riesgos\*\*: Evaluar el riesgo de incumplimiento y establecer medidas preventivas para evitar recargos.

## 3.4 Cumplimiento de Requisitos de Datos

* \*\*Actualización de Procesos\*\*: Asegurar que los procesos de transacción incluyan la dirección del destinatario en AFT a partir de la fecha establecida.

## 4. Riesgos y Consecuencias del Incumplimiento

## 4.1 Riesgos Financieros

* \*\*Recargos por Incumplimiento\*\*: Comercios de Nivel 3 enfrentarán recargos escalonados que pueden impactar significativamente sus márgenes de ganancia.

## 4.2 Riesgos Legales

* \*\*Sanciones Regulatorias\*\*: El incumplimiento de las normativas de VISA puede resultar en sanciones legales y pérdida de la capacidad de procesar pagos a través de la red de VISA.

## 4.3 Riesgos de Reputación

* \*\*Pérdida de Confianza del Consumidor\*\*: Los incidentes de seguridad pueden dañar la reputación de los comercios, afectando la confianza del consumidor y, en consecuencia, las ventas.

## 4.4 Riesgos Operativos

* \*\*Interrupciones en el Servicio\*\*: La falta de cumplimiento puede llevar a interrupciones en el servicio de procesamiento de pagos, afectando la operativa diaria del comercio.

## Conclusión

Las nuevas reglas de seguridad de VISA representan un esfuerzo significativo para mejorar la seguridad en el ecosistema de pagos electrónicos. Es crucial que los comercios y adquirentes se adapten a estas normativas para evitar riesgos financieros, legales y operativos. La implementación efectiva de los procesos de cumplimiento y la capacitación del personal son esenciales para garantizar la continuidad y seguridad dentro de la red de VISA.

# 4. Conclusiones

## Conclusiones Clave sobre el Análisis Normativo de las Nuevas Reglas de Seguridad de VISA

1. \*\*Fortalecimiento de la Seguridad en Transacciones Electrónicas\*\*: Las nuevas reglas de VISA, a través de la implementación de extensiones de mensaje y requisitos de seguridad de la información, buscan robustecer la protección de datos en el ecosistema de pagos. Esto es fundamental para mitigar el riesgo de fraudes y proteger la información sensible de los consumidores.

2. \*\*Obligaciones Claras para Comercios y Adquirentes\*\*: La normativa establece obligaciones específicas que los comercios y adquirentes deben cumplir, como la implementación de las nuevas extensiones de mensaje y el cumplimiento con PCI DSS. Esto implica que las entidades deben realizar inversiones en tecnología y capacitación para cumplir con los estándares requeridos.

3. \*\*Impacto Financiero por Incumplimiento\*\*: Los recargos escalonados por incumplimiento para comercios de Nivel 3 pueden tener un impacto significativo en la rentabilidad de estos negocios. Es esencial que los comercios evalúen sus procesos internos y establezcan medidas preventivas para evitar sanciones económicas.

4. \*\*Riesgos Legales y de Reputación\*\*: El incumplimiento de las normativas de VISA no solo puede resultar en sanciones legales, sino que también puede dañar la reputación de los comercios. La confianza del consumidor es un activo valioso, y cualquier incidente de seguridad puede llevar a una pérdida de clientes y a un deterioro de la imagen de marca.

5. \*\*Necesidad de Auditorías y Controles Internos\*\*: La implementación de auditorías internas y controles de acceso estrictos es crucial para garantizar el cumplimiento continuo con las normativas. Esto no solo ayuda a prevenir el incumplimiento, sino que también fortalece la cultura de seguridad dentro de la organización.

6. \*\*Preparación para Cambios Futuro\*\*: La inclusión obligatoria del campo de dirección del destinatario en transacciones AFT transfronterizas a partir de julio de 2025 es un cambio significativo que requiere preparación anticipada. Los comercios deben actualizar sus sistemas y procesos para cumplir con esta nueva exigencia.

7. \*\*Capacitación del Personal como Pilar Fundamental\*\*: La capacitación del personal en las nuevas especificaciones y en la importancia de la seguridad de la información es esencial. Un equipo bien informado y preparado es clave para la implementación exitosa de las nuevas normativas y para la protección de la información del cliente.

8. \*\*Gestión Proactiva de Riesgos\*\*: La evaluación de riesgos y la implementación de medidas preventivas son fundamentales para evitar no solo recargos, sino también interrupciones en el servicio de procesamiento de pagos. La gestión proactiva de riesgos puede ayudar a los comercios a mantener la continuidad operativa y a proteger su reputación.

En resumen, las nuevas reglas de seguridad de VISA son un paso importante hacia la mejora de la seguridad en el comercio electrónico. Sin embargo, requieren un compromiso significativo por parte de los comercios y adquirentes para garantizar su cumplimiento y proteger tanto sus operaciones como la confianza de sus clientes.

# 5. Recomendaciones

A continuación, se presentan recomendaciones prácticas y accionables para que los comercios y adquirentes cumplan con las nuevas reglas de seguridad de VISA:

## Recomendaciones Prácticas para el Cumplimiento de las Nuevas Reglas de Seguridad de VISA

## 1. \*\*Evaluación de Infraestructura Tecnológica\*\*

* Realizar un inventario completo de los sistemas y tecnologías actuales utilizados en el procesamiento de pagos.
* Identificar las brechas de cumplimiento con las nuevas extensiones de mensaje y los requisitos de PCI DSS.
* Planificar actualizaciones tecnológicas necesarias para cumplir con las normativas.

## 2. \*\*Implementación de Extensiones de Mensaje\*\*

* Desarrollar un plan de implementación para las nuevas extensiones de mensaje, asegurando que todos los sistemas de pago estén actualizados.
* Realizar pruebas exhaustivas para garantizar que las extensiones se integren correctamente en el flujo de transacciones.

## 3. \*\*Capacitación y Concienciación del Personal\*\*

* Desarrollar un programa de capacitación regular sobre las nuevas normativas y la importancia de la seguridad de la información.
* Incluir simulaciones de incidentes de seguridad para preparar al personal en la respuesta ante posibles brechas de seguridad.

## 4. \*\*Establecimiento de Controles Internos y Auditorías\*\*

* Implementar controles de acceso estrictos y políticas de seguridad de la información que regulen quién puede acceder a datos sensibles.
* Programar auditorías internas periódicas para evaluar el cumplimiento con las normativas y la efectividad de los controles implementados.

## 5. \*\*Gestión de Riesgos\*\*

* Realizar una evaluación de riesgos integral que identifique vulnerabilidades en los procesos de pago y en la protección de datos.
* Desarrollar un plan de gestión de riesgos que incluya medidas preventivas y protocolos de respuesta ante incidentes.

## 6. \*\*Preparación para Cambios Futuros\*\*

* Establecer un equipo de proyecto dedicado a la implementación de cambios normativos, como la inclusión del campo de dirección del destinatario en transacciones AFT.
* Iniciar la actualización de sistemas y procesos con anticipación para cumplir con la fecha límite de julio de 2025.

## 7. \*\*Monitoreo Continuo y Mejora\*\*

* Implementar un sistema de monitoreo continuo para detectar y responder a posibles incidentes de seguridad en tiempo real.
* Fomentar una cultura de mejora continua en la seguridad de la información, revisando y actualizando políticas y procedimientos regularmente.

## 8. \*\*Comunicación Transparente con Clientes\*\*

* Informar a los clientes sobre las medidas de seguridad implementadas y cómo se protege su información.
* Establecer canales de comunicación para que los clientes puedan reportar incidentes o preocupaciones de seguridad.

## 9. \*\*Colaboración con Proveedores y Socios\*\*

* Trabajar en estrecha colaboración con proveedores de servicios de pago y tecnología para asegurar que también cumplan con las nuevas normativas.
* Realizar revisiones de cumplimiento con socios comerciales para garantizar que todos los aspectos de la cadena de suministro estén alineados con las regulaciones.

## 10. \*\*Documentación y Reportes\*\*

* Mantener una documentación exhaustiva de todos los procesos, políticas y auditorías relacionadas con el cumplimiento de las normativas de VISA.
* Establecer un sistema de reportes que permita a la alta dirección monitorear el estado de cumplimiento y las medidas de seguridad implementadas.

Al seguir estas recomendaciones, los comercios y adquirentes no solo cumplirán con las nuevas reglas de seguridad de VISA, sino que también fortalecerán su postura de seguridad general, protegiendo así tanto sus operaciones como la confianza de sus clientes.

# 6. Referencias

Para la sección de referencias del informe sobre las nuevas reglas de seguridad de VISA para comercios electrónicos, se deben incluir las siguientes fuentes y documentos oficiales relevantes:

## 1. \*\*Documentación de VISA sobre Seguridad de Pagos\*\*

* Publicaciones oficiales de VISA relacionadas con la seguridad de transacciones electrónicas, incluyendo guías y especificaciones técnicas.

## 2. \*\*Visa Secure\*\*

* Documentación específica sobre el programa Visa Secure, que detalla las medidas de seguridad y autenticación para transacciones en línea.

## 3. \*\*Evidencia Convincente 3.0 (CE3.0)\*\*

* Documentos que describen las características y requisitos de la versión 3.0 de Evidencia Convincente, que es parte de las medidas de seguridad de VISA.

## 4. \*\*Intercambio de Datos Inteligentes (IDX)\*\*

* Información sobre el sistema IDX y su función en la mejora de la seguridad de las transacciones y la prevención del fraude.

## 5. \*\*Normativas de la Industria de Tarjetas de Pago (PCI DSS)\*\*

* Referencias a las normativas de seguridad de datos de la industria de tarjetas de pago, que son relevantes para la implementación de medidas de seguridad en comercios electrónicos.

## 6. \*\*Especificaciones de Mensaje Globales de VISA\*\*

* Documentación que detalla las especificaciones de mensajes globales, incluyendo las nuevas extensiones de datos (VAD y VPDE).

## 7. \*\*Comunicados de Prensa de VISA\*\*

* Comunicados oficiales que anuncian la publicación y habilitación de nuevas reglas y especificaciones.

## 8. \*\*Regulaciones Locales y Internacionales\*\*

* Cualquier normativa local o internacional que pueda afectar la implementación de las nuevas reglas de seguridad en diferentes jurisdicciones.

Incluir estas referencias proporcionará un contexto adecuado y respaldará la información presentada en el informe.