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

Análisis y Recomendaciones para la Implementación de las Últimas Regulaciones en el Comercio Digital

26/04/2025

# 1. Executive Summary

* Ejecutivo:\*\*

El análisis normativo sobre las nuevas reglas de seguridad de Visa para comercios electrónicos, actualizado en octubre de 2024, destaca cambios significativos en la autenticación y protección contra el fraude en transacciones electrónicas. Se introducen nuevas ediciones de los documentos Visa Core Rules y Visa Merchant Data Standards Manual, con el objetivo de fortalecer la seguridad del ecosistema de pagos. A partir del 15 de abril de 2025, se implementarán las extensiones de mensajes Visa Additional Data y Visa Program Data, que mejorarán la autenticación y la conformidad de las transacciones. Además, desde el 11 de julio de 2025, se exigirá que los adquirentes incluyan la dirección del destinatario en transferencias AFT transfronterizas, y a partir del 17 de octubre de 2025, se denegarán transacciones sin la información requerida del remitente. Estas medidas reflejan el compromiso de Visa por mejorar la seguridad y la integridad en el comercio electrónico.

# 2. Alcance

## Alcance del Informe

El presente informe tiene como objetivo proporcionar un análisis exhaustivo de las nuevas reglas de seguridad de Visa para comercios electrónicos, con un enfoque particular en las actualizaciones más recientes y su impacto en la autenticación y seguridad de las transacciones electrónicas. Este informe se basa en la información más actualizada disponible hasta octubre de 2023 y se centra en las siguientes áreas clave:

1. \*\*Actualizaciones Normativas\*\*: Se detallarán las modificaciones introducidas en las ediciones de octubre de 2024 de los documentos Visa Core Rules, Visa Product and Service Rules, y Visa Merchant Data Standards Manual, así como su propósito de mejorar la seguridad y protección contra el fraude.

2. \*\*Implementación de Visa Secure\*\*: Se analizarán las nuevas extensiones de mensajes globales, incluyendo la Visa Additional Data Extension y la Visa Program Data Extension, que entrarán en vigor el 15 de abril de 2025, y su relevancia para los comercios electrónicos.

3. \*\*Impacto en Comercios Electrónicos\*\*: Se evaluará cómo estas nuevas reglas afectan a los comercios electrónicos en términos de cumplimiento normativo, procedimientos de autenticación y medidas de seguridad que deben implementarse para proteger tanto a los comerciantes como a los consumidores.

4. \*\*Limitaciones del Informe\*\*: Este informe no abordará aspectos relacionados con la implementación técnica específica de las nuevas reglas en plataformas de comercio electrónico, ni se centrará en casos de uso individuales o en la experiencia de usuarios finales. Además, se limita a la normativa vigente hasta octubre de 2023 y no incluirá cambios o actualizaciones posteriores a esta fecha.

El informe está diseñado para ser una herramienta informativa para comerciantes, desarrolladores de sistemas de pago y profesionales de la seguridad, facilitando una comprensión clara de las nuevas exigencias de Visa y su aplicación en el entorno del comercio electrónico.

# 3. Análisis Regulatorio

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

Este análisis regulatorio se centra en las actualizaciones recientes de Visa en relación con la seguridad y autenticación en transacciones electrónicas, tal como se detalla en la información proporcionada. Se estructurará en varias subsecciones que abordan los principales requisitos normativos, las obligaciones para las entidades reguladas, los procesos de cumplimiento necesarios, así como los riesgos y consecuencias del incumplimiento.

## 1. Principales Requisitos Normativos Identificados

## 1.1 Actualización de Documentos Normativos

* \*\*Documentos Clave\*\*: Visa Core Rules, Visa Product and Service Rules, y Visa Merchant Data Standards Manual (Edición octubre 2024).
* \*\*Objetivo\*\*: Mejorar la seguridad de las transacciones y la protección contra el fraude.

## 1.2 Nuevas Extensiones de Mensaje Globales

* \*\*Visa Additional Data Extension\*\*: Implementación el 15 de abril de 2025, para soportar programas de autenticación como Compelling Evidence 3.0.
* \*\*Visa Program Data Extension\*\*: Proporciona información sobre la conformidad de las transacciones con los programas de autenticación de Visa.

## 1.3 Requisitos de Campos de Datos

* \*\*Campo de Dirección del Destinatario\*\*: Obligatorio a partir del 11 de julio de 2025 para transferencias AFT transfronterizas a Australia, Nueva Zelanda y el Pacífico Sur.
* \*\*Denegación de Transacciones\*\*: A partir del 17 de octubre de 2025, las transacciones sin los campos requeridos (nombre, dirección del remitente, origen de fondos) serán rechazadas.

## 1.4 Actualizaciones del Documento 'What To Do If Compromised'

* \*\*Recargos por Incumplimiento\*\*: Nuevos recargos escalonados para comercios de Nivel 3.
* \*\*Cumplimiento PCI DSS\*\*: Se mantiene el requerimiento de cumplimiento de normas de seguridad para todas las entidades que manejan datos de tarjetas de crédito.

## 1.5 Control de Sanciones

* \*\*Revisión de Sanciones\*\*: Obligación de revisar y controlar si los tarjetahabientes y comercios figuran en listas de sanciones aplicables.

## 1.6 Eliminación del Requisito CAID Único

* \*\*Identificación\*\*: Se elimina la necesidad de un identificador único para ciertos comercios, alineándose con el Global Acceptor Identification Framework.

## 2. Obligaciones para las Entidades Reguladas

## 2.1 Adquirentes y Comercios

* \*\*Adaptación a Nuevas Normas\*\*: Deben actualizar sus sistemas y procesos para cumplir con las nuevas reglas antes de las fechas de implementación.
* \*\*Cumplimiento de Requisitos de Datos\*\*: Asegurar que se completen todos los campos requeridos en las transacciones.

## 2.2 Revisión de Sanciones

* \*\*Diligencia Debida\*\*: Implementar procesos para verificar que no haya coincidencias con listas de sanciones.

## 2.3 Cumplimiento de PCI DSS

* \*\*Seguridad de Datos\*\*: Mantener los estándares de seguridad requeridos para la protección de datos de tarjetas de crédito.

## 3. Procesos de Cumplimiento Necesarios

## 3.1 Implementación de Sistemas de Autenticación

* \*\*Integración de Nuevas Extensiones\*\*: Adaptar los sistemas de pago para incluir las nuevas extensiones de mensajes de Visa.

## 3.2 Capacitación y Concienciación

* \*\*Formación del Personal\*\*: Capacitar a los empleados sobre las nuevas normas y procedimientos de seguridad.

## 3.3 Auditorías Internas

* \*\*Revisión de Cumplimiento\*\*: Realizar auditorías internas periódicas para asegurar que se cumplan las nuevas regulaciones y estándares.

## 3.4 Monitoreo Continuo

* \*\*Vigilancia de Transacciones\*\*: Implementar sistemas de monitoreo para detectar y prevenir fraudes en tiempo real.

## 4. Riesgos y Consecuencias del Incumplimiento

## 4.1 Riesgos Financieros

* \*\*Denegación de Transacciones\*\*: Las transacciones que no cumplan con los requisitos serán rechazadas, lo que puede resultar en pérdidas significativas de ingresos.

## 4.2 Sanciones y Multas

* \*\*Recargos por Incumplimiento\*\*: Los comercios de Nivel 3 enfrentarán recargos escalonados si no cumplen con las nuevas normas.

## 4.3 Daño a la Reputación

* \*\*Pérdida de Confianza\*\*: El incumplimiento puede llevar a una pérdida de confianza por parte de los consumidores y socios comerciales.

## 4.4 Consecuencias Legales

* \*\*Acciones Legales\*\*: Posibles acciones legales por parte de consumidores o entidades reguladoras en caso de violaciones de seguridad.

## Conclusión

Las nuevas reglas y estándares de Visa están diseñados para fortalecer la seguridad en el comercio electrónico y combatir el fraude. Es esencial que los adquirentes y comercios implementen estas actualizaciones de manera efectiva antes de las fechas de vencimiento establecidas. La falta de cumplimiento no solo puede resultar en pérdidas financieras, sino también en sanciones severas y daños a la reputación. Se recomienda a las entidades reguladas que consulten regularmente los recursos de Visa para mantenerse actualizadas y alineadas con las normativas vigentes.

# 4. Conclusiones

## Conclusiones Clave sobre el Análisis Normativo de las Nuevas Reglas de Seguridad de Visa para Comercios Electrónicos

1. \*\*Fortalecimiento de la Seguridad en Transacciones\*\*: Las actualizaciones de Visa reflejan un enfoque proactivo hacia la mejora de la seguridad en las transacciones electrónicas. La implementación de nuevas extensiones de mensajes y requisitos de datos obligatorios es un paso crucial para mitigar el riesgo de fraude y proteger tanto a los consumidores como a los comerciantes.

2. \*\*Obligaciones Claras para Entidades Reguladas\*\*: Las entidades reguladas, incluidos adquirentes y comercios, tienen la responsabilidad de adaptarse a las nuevas normas. Esto implica no solo la actualización de sistemas y procesos, sino también la capacitación del personal y la implementación de auditorías internas. La diligencia debida en la revisión de sanciones es igualmente crítica para evitar complicaciones legales.

3. \*\*Riesgos Financieros y Reputacionales\*\*: El incumplimiento de las nuevas regulaciones puede acarrear consecuencias financieras significativas, incluyendo la denegación de transacciones y recargos escalonados. Además, el daño a la reputación de los comercios puede ser devastador, afectando la confianza del consumidor y las relaciones comerciales.

4. \*\*Importancia del Cumplimiento Continuo\*\*: La normativa no solo exige una adaptación inicial, sino que también requiere un compromiso continuo con el cumplimiento. Esto incluye la vigilancia activa de las transacciones y la actualización constante de los procedimientos de seguridad para alinearse con las mejores prácticas y estándares de la industria.

5. \*\*Implicaciones Legales Potenciales\*\*: Las nuevas reglas también abren la puerta a posibles acciones legales en caso de violaciones de seguridad. Las entidades deben ser conscientes de las implicaciones legales que pueden surgir de un incumplimiento, lo que subraya la necesidad de un enfoque riguroso hacia la conformidad normativa.

6. \*\*Recomendaciones para la Implementación\*\*: Se sugiere que las entidades reguladas establezcan un plan de acción claro que incluya la evaluación de sus sistemas actuales, la identificación de brechas en el cumplimiento, y la asignación de recursos adecuados para la capacitación y la implementación de nuevas tecnologías de seguridad.

7. \*\*Consulta Continua con Recursos de Visa\*\*: Para mantenerse al día con las normativas y adaptarse a futuros cambios, es fundamental que las entidades reguladas consulten regularmente los recursos y actualizaciones proporcionados por Visa. Esto les permitirá no solo cumplir con las normativas vigentes, sino también anticipar y prepararse para futuras exigencias regulatorias.

En resumen, la adaptación a las nuevas reglas de Visa es un imperativo estratégico para los comercios electrónicos. La implementación efectiva de estas normativas no solo protegerá a las entidades de riesgos financieros y legales, sino que también contribuirá a la creación de un entorno de comercio electrónico más seguro y confiable.

# 5. Recomendaciones

A continuación, se presentan recomendaciones prácticas y accionables para el cumplimiento de las nuevas reglas de seguridad de Visa para comercios electrónicos, basadas en el análisis normativo y las conclusiones clave:

## Recomendaciones Prácticas para el Cumplimiento Normativo

## 1. \*\*Evaluación de Sistemas Actuales\*\*

* Realizar una auditoría exhaustiva de los sistemas de procesamiento de pagos actuales para identificar brechas en el cumplimiento con las nuevas normas de Visa.
* Documentar los hallazgos y priorizar las áreas que requieren atención inmediata.

## 2. \*\*Actualización de Tecnología\*\*

* Invertir en tecnologías de seguridad avanzadas, como la autenticación multifactor (MFA), cifrado de datos y sistemas de detección de fraudes en tiempo real.
* Asegurarse de que todos los sistemas de pago estén actualizados y sean compatibles con las nuevas extensiones de mensajes y requisitos de datos obligatorios.

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

* Desarrollar un programa de capacitación integral para todos los empleados, enfocado en las nuevas regulaciones de Visa, la seguridad de datos y la prevención del fraude.
* Realizar sesiones de capacitación periódicas para mantener al personal informado sobre las mejores prácticas y cambios normativos.

## 4. \*\*Implementación de Auditorías Internas\*\*

* Establecer un calendario regular para auditorías internas que evalúen el cumplimiento de las nuevas normas y la eficacia de las medidas de seguridad implementadas.
* Incluir revisiones de procesos y procedimientos para garantizar que se sigan las mejores prácticas en la gestión de transacciones.

## 5. \*\*Desarrollo de un Plan de Respuesta a Incidentes\*\*

* Crear un plan de respuesta a incidentes que detalle los pasos a seguir en caso de una violación de seguridad, incluyendo la notificación a las partes afectadas y a las autoridades pertinentes.
* Realizar simulacros de respuesta a incidentes para asegurar que el personal esté preparado para actuar de manera efectiva.

## 6. \*\*Monitoreo Continuo de Transacciones\*\*

* Implementar sistemas de monitoreo continuo que analicen las transacciones en tiempo real para detectar actividades sospechosas o inusuales.
* Establecer alertas automáticas para notificar al personal de seguridad sobre transacciones que puedan requerir una revisión adicional.

## 7. \*\*Documentación y Registro\*\*

* Mantener registros detallados de todas las transacciones, auditorías y capacitaciones realizadas para demostrar el cumplimiento con las normativas de Visa.
* Asegurarse de que la documentación esté fácilmente accesible para auditorías externas o revisiones regulatorias.

## 8. \*\*Consulta Regular con Recursos de Visa\*\*

* Designar un equipo o persona responsable de mantenerse actualizado con las últimas normativas y recursos proporcionados por Visa.
* Participar en seminarios web, talleres y conferencias organizadas por Visa para obtener información sobre las mejores prácticas y cambios en la normativa.

## 9. \*\*Evaluación de Riesgos Legales\*\*

* Consultar con asesores legales para evaluar las implicaciones legales de las nuevas regulaciones y desarrollar estrategias para mitigar riesgos potenciales.
* Considerar la posibilidad de contratar un seguro de responsabilidad cibernética para protegerse contra posibles reclamaciones legales.

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

* Informar a los clientes sobre las medidas de seguridad implementadas y cómo se protege su información personal y financiera.
* Fomentar la confianza del consumidor mediante la transparencia en las políticas de privacidad y seguridad.

## Conclusión

La implementación de estas recomendaciones no solo ayudará a los comercios electrónicos a cumplir con las nuevas reglas de Visa, sino que también fortalecerá la seguridad general de las transacciones y mejorará la confianza del consumidor. Un enfoque proactivo y sistemático es esencial para navegar el panorama regulatorio en constante evolución y proteger tanto a los consumidores como a las entidades reguladas.

# 6. Referencias

Para la sección de referencias del análisis normativo sobre las nuevas reglas de seguridad de Visa para comercios electrónicos, se deben incluir los siguientes documentos y fuentes oficiales mencionadas:

1. \*\*Visa Core Rules\*\* - Edición de octubre 2024. 2. \*\*Visa Product and Service Rules\*\* - Edición de octubre 2024. 3. \*\*Visa Merchant Data Standards Manual\*\* - Edición de octubre 2024. 4. \*\*Visa Secure\*\* - Documentación relacionada con las nuevas extensiones de mensajes globales, incluyendo: - \*\*Visa Additional Data Extension\*\* - \*\*Visa Program Data Extension\*\* - Fecha de implementación: 15 de abril de 2025.

Es recomendable que se verifique la disponibilidad de estos documentos en el sitio oficial de Visa o en la plataforma de recursos para comerciantes de Visa, para asegurar que se está utilizando la información más actualizada y precisa.