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

Análisis y Recomendaciones para la Implementación de las Directrices Actualizadas

27/04/2025

# 1. Executive Summary

* Ejecutivo:\*\*

El informe detalla las actualizaciones de seguridad de VISA para comercios electrónicos, con énfasis en las nuevas reglas que entrarán en vigor a partir de octubre de 2024. Se destacan las nuevas extensiones de mensaje globales, como la Visa Additional Data Extension y la Visa Program Data Extension, que se implementarán el 15 de abril de 2025, con requisitos de intercambio de datos para mejorar la autenticación y seguridad en transacciones. Además, se establecen nuevas pautas para la respuesta a compromisos de seguridad y recargos por incumplimiento para comercios de Nivel 3, vigentes desde el 9 de febrero de 2025. A partir del 11 de julio de 2025, se requerirán nuevos campos de datos para transacciones AFT y OCT, y se introducirán reglas para rechazar transacciones no conformes a partir del 17 de octubre de 2025. Es crucial que los adquirentes, procesadores y emisores revisen el Resumen de Cambios para adaptarse a estos nuevos requisitos.

# 2. Alcance

## Alcance del Informe

El presente informe tiene como propósito proporcionar un análisis exhaustivo de las nuevas reglas de seguridad de VISA aplicables a los comercios electrónicos, con un enfoque en las actualizaciones más recientes y su impacto en los actores del ecosistema de pagos. Este documento está diseñado para ser una guía informativa para adquirentes, procesadores, emisores y comerciantes que operan en el ámbito del comercio electrónico.

## Objetivos Específicos

1. \*\*Describir las Actualizaciones Generales de Seguridad:\*\* Se abordarán las modificaciones introducidas en las reglas de VISA, destacando los cambios más relevantes y su implicación para los diferentes participantes en el proceso de pago.

2. \*\*Analizar las Nuevas Extensiones de Mensaje Globales:\*\* Se detallarán las especificaciones de las nuevas extensiones de mensaje, como la Visa Additional Data Extension y la Visa Program Data Extension, y su relevancia en la mejora de la seguridad de las transacciones en línea.

3. \*\*Proporcionar Fechas Clave y Requisitos de Implementación:\*\* Se incluirán las fechas de implementación de las nuevas reglas y cualquier requisito adicional que los comercios electrónicos deban cumplir para alinearse con las normativas de VISA.

## Límites del Informe

* \*\*Temporalidad:\*\* El informe se basa en la documentación y actualizaciones disponibles hasta octubre de 2024, y considera las fechas de implementación futuras hasta abril de 2025.
* \*\*Enfoque en Comercio Electrónico:\*\* Aunque se mencionan aspectos generales de seguridad, el informe se centra exclusivamente en las reglas aplicables a los comercios electrónicos, sin abordar otros segmentos del mercado de pagos.
* \*\*Exclusión de Análisis de Competencia:\*\* Este informe no incluye comparaciones con las normativas de otras entidades de pago o competidores en el sector, centrándose únicamente en las directrices de VISA.

Este alcance establece un marco claro para la comprensión de las nuevas reglas de seguridad de VISA, permitiendo a los interesados tomar decisiones informadas y adecuarse a las normativas vigentes en el 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 Actualizaciones Generales de Seguridad

* \*\*Documentación:\*\* Las nuevas reglas se encuentran en las ediciones de octubre de 2024 de Visa Core Rules y Visa Product and Service Rules.
* \*\*Impacto:\*\* Estas actualizaciones afectan a adquirentes, procesadores y emisores, quienes deben revisar el Resumen de Cambios para entender los nuevos requisitos.

## 1.2 Visa Secure: Nuevas Extensiones de Mensaje Globales

* \*\*Fecha de Implementación:\*\* 15 de abril de 2025.
* \*\*Especificaciones Clave:\*\*
* \*\*Visa Additional Data Extension:\*\* Requiere que los comercios envíen datos adicionales para mejorar la seguridad en las transacciones.
* \*\*Visa Program Data Extension:\*\* Obliga a los comercios a proporcionar información sobre el cumplimiento de programas de autenticación.

## 1.3 Cambios en los Requisitos de Datos

* \*\*Transacciones AFT y OCT:\*\* A partir del 11 de julio de 2025, los comercios deberán incluir nuevos campos de datos, como la dirección del destinatario.
* \*\*Rechazo de Transacciones:\*\* Desde el 17 de octubre de 2025, se implementarán reglas para rechazar transacciones que no cumplan con los nuevos requisitos de datos.

## 1.4 Control de Sanciones

* \*\*Verificación Obligatoria:\*\* Los comercios deben asegurarse de que tanto los tarjetahabientes como ellos mismos no estén en listas de sanciones aplicables, tomando medidas adecuadas en caso de coincidencias.

## 2. Obligaciones para las Entidades Reguladas

## 2.1 Adquirentes, Procesadores y Emisores

* \*\*Revisión de Documentación:\*\* Deben revisar y comprender las actualizaciones en Visa Core Rules y Visa Product and Service Rules.
* \*\*Implementación de Nuevas Especificaciones:\*\* Deben estar preparados para implementar las nuevas extensiones de mensaje globales y cumplir con los requisitos de datos adicionales.

## 2.2 Comercios Electrónicos

* \*\*Envío de Datos Adicionales:\*\* Aunque el intercambio de datos es opcional, ciertos datos serán obligatorios para cumplir con los estándares de seguridad.
* \*\*Cumplimiento de Nuevos Campos de Datos:\*\* Deben asegurarse de que las transacciones AFT y OCT incluyan la dirección del destinatario a partir del 11 de julio de 2025.

## 2.3 Protocolo de Respuesta a Compromisos de Seguridad

* \*\*Actualización de Protocolos:\*\* Los comercios deben seguir las nuevas directrices sobre cómo actuar en caso de compromisos de seguridad, incluyendo la implementación de recargos por incumplimiento.

## 3. Procesos de Cumplimiento Necesarios

## 3.1 Capacitación y Concienciación

* \*\*Formación del Personal:\*\* Es esencial que el personal de los comercios y entidades reguladas reciba capacitación sobre las nuevas reglas y procedimientos de seguridad.

## 3.2 Implementación de Sistemas Tecnológicos

* \*\*Actualización de Sistemas:\*\* Los comercios deben actualizar sus sistemas de procesamiento de pagos para incluir los nuevos campos de datos y cumplir con las extensiones de mensaje globales.

## 3.3 Monitoreo y Verificación

* \*\*Control de Sanciones:\*\* Establecer un sistema de monitoreo para verificar que los tarjetahabientes y comercios no estén en listas de sanciones aplicables.

## 3.4 Auditorías Internas

* \*\*Revisiones Periódicas:\*\* Realizar auditorías internas para asegurar el cumplimiento continuo de las nuevas regulaciones y protocolos de seguridad.

## 4. Riesgos y Consecuencias del Incumplimiento

## 4.1 Riesgos Financieros

* \*\*Recargos por Incumplimiento:\*\* Los comercios de Nivel 3 enfrentarán nuevos recargos por incumplimiento a partir del 9 de febrero de 2025, lo que puede impactar significativamente sus márgenes de ganancia.

## 4.2 Riesgos de Seguridad

* \*\*Compromisos de Seguridad:\*\* El incumplimiento de las nuevas reglas puede aumentar la vulnerabilidad a fraudes y compromisos de seguridad, lo que podría resultar en pérdidas financieras y daños a la reputación.

## 4.3 Consecuencias Legales

* \*\*Sanciones Regulatorias:\*\* Las entidades que no cumplan con las nuevas regulaciones pueden enfrentar sanciones legales y regulatorias, así como la pérdida de la capacidad para procesar pagos a través de VISA.

## 4.4 Impacto en la Confianza del Consumidor

* \*\*Pérdida de Clientes:\*\* La falta de cumplimiento puede llevar a la pérdida de confianza por parte de los consumidores, lo que podría resultar en una disminución de las ventas y la lealtad del cliente.

## Conclusión

Las nuevas reglas de seguridad de VISA para comercios electrónicos representan un cambio significativo en el panorama de la seguridad de pagos. Es crucial que las entidades reguladas se preparen adecuadamente para cumplir con estos requisitos, implementando procesos y sistemas que garanticen la seguridad y la autenticidad en las transacciones. La falta de cumplimiento no solo conlleva riesgos financieros y legales, sino que también puede afectar la confianza del consumidor y la reputación del comercio.

# 4. Conclusiones

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

1. \*\*Urgencia en la Adaptación a Nuevas Normativas:\*\* Las actualizaciones en las reglas de VISA, que entrarán en vigor en fechas específicas hasta 2025, requieren que las entidades reguladas (adquirentes, procesadores y emisores) y los comercios electrónicos actúen con rapidez para revisar y adaptar sus sistemas y procesos. La falta de preparación puede resultar en sanciones financieras y operativas significativas.

2. \*\*Enfoque en la Seguridad de Datos:\*\* La implementación de la Visa Additional Data Extension y la Visa Program Data Extension subraya la importancia de la seguridad en las transacciones. Los comercios deben asegurarse de que los datos adicionales sean enviados correctamente para mitigar riesgos de fraude y cumplir con los estándares de VISA. Esto implica no solo cambios técnicos, sino también un cambio cultural hacia la seguridad de datos.

3. \*\*Cumplimiento Obligatorio de Nuevos Requisitos:\*\* A partir de las fechas establecidas, los comercios deberán incluir nuevos campos de datos en las transacciones AFT y OCT, así como verificar que no estén en listas de sanciones. La implementación de estos requisitos es crítica para evitar el rechazo de transacciones y otros problemas operativos.

4. \*\*Riesgos Financieros y de Reputación:\*\* Los comercios de Nivel 3 enfrentarán recargos por incumplimiento, lo que puede impactar negativamente sus márgenes de ganancia. Además, el incumplimiento puede resultar en compromisos de seguridad que no solo afectan las finanzas, sino que también dañan la reputación del comercio y la confianza del consumidor.

5. \*\*Necesidad de Capacitación y Concienciación:\*\* La formación del personal es esencial para garantizar que todos los involucrados comprendan las nuevas reglas y procedimientos de seguridad. Esto no solo ayuda a cumplir con las normativas, sino que también fomenta una cultura organizacional centrada en la seguridad.

6. \*\*Implementación de Sistemas Tecnológicos:\*\* La actualización de los sistemas de procesamiento de pagos es fundamental para cumplir con las nuevas especificaciones. Esto incluye la integración de nuevos campos de datos y la adopción de tecnologías que faciliten el cumplimiento normativo.

7. \*\*Monitoreo Continuo y Auditorías:\*\* Establecer un sistema de monitoreo para verificar el cumplimiento de las listas de sanciones y realizar auditorías internas periódicas son prácticas necesarias para asegurar que las entidades reguladas mantengan estándares de seguridad y cumplimiento a largo plazo.

8. \*\*Implicaciones Legales y Regulatorias:\*\* Las entidades que no cumplan con las nuevas regulaciones pueden enfrentar sanciones legales y la pérdida de la capacidad para procesar pagos a través de VISA. Esto resalta la importancia de la conformidad no solo desde una perspectiva operativa, sino también legal.

9. \*\*Impacto en la Confianza del Consumidor:\*\* La falta de cumplimiento puede llevar a la pérdida de confianza por parte de los consumidores, lo que puede traducirse en una disminución de las ventas y la lealtad del cliente. Por lo tanto, el cumplimiento normativo no solo es una cuestión de evitar sanciones, sino también de mantener la relación con los clientes.

En resumen, las nuevas reglas de seguridad de VISA representan un desafío significativo para los comercios electrónicos y las entidades reguladas. La preparación adecuada, la implementación de sistemas robustos y la formación del personal son esenciales para garantizar el cumplimiento y la seguridad en las transacciones, así como para proteger la confianza del consumidor y la reputación del comercio.

# 5. Recomendaciones

A continuación, se presentan recomendaciones prácticas y accionables para ayudar a los comercios electrónicos y entidades reguladas a cumplir con las nuevas reglas de seguridad de VISA:

## Recomendaciones Prácticas para el Cumplimiento Normativo

1. \*\*Desarrollo de un Plan de Acción:\*\* - \*\*Establecer un cronograma\*\* con fechas límite para la revisión y adaptación de sistemas y procesos en función de las fechas de entrada en vigor de las nuevas normativas. - \*\*Asignar responsabilidades\*\* a equipos específicos para cada aspecto del cumplimiento normativo.

2. \*\*Evaluación de Sistemas Actuales:\*\* - Realizar un \*\*análisis de brechas\*\* para identificar las áreas donde los sistemas actuales no cumplen con los nuevos requisitos de VISA. - \*\*Actualizar o reemplazar\*\* los sistemas de procesamiento de pagos que no puedan adaptarse a las nuevas especificaciones.

3. \*\*Implementación de Nuevos Campos de Datos:\*\* - Integrar los nuevos campos de datos requeridos en las transacciones AFT y OCT en los sistemas de pago. - Asegurarse de que los sistemas puedan manejar la \*\*validación y el envío correcto\*\* de estos datos adicionales.

4. \*\*Verificación de Listas de Sanciones:\*\* - Implementar un sistema automatizado para verificar que las transacciones no involucren a entidades en listas de sanciones. - Establecer procedimientos para manejar transacciones que sean rechazadas por estar en estas listas.

5. \*\*Capacitación del Personal:\*\* - Desarrollar un programa de \*\*formación continua\*\* sobre las nuevas normativas y procedimientos de seguridad para todos los empleados, especialmente aquellos en áreas de finanzas y tecnología. - Realizar \*\*talleres y simulaciones\*\* para preparar al personal ante situaciones de incumplimiento o fraude.

6. \*\*Cultura de Seguridad de Datos:\*\* - Fomentar una cultura organizacional que priorice la \*\*seguridad de datos\*\* mediante la comunicación regular sobre la importancia del cumplimiento normativo. - Implementar políticas de seguridad que incluyan la \*\*protección de datos sensibles\*\* y la respuesta ante incidentes.

7. \*\*Monitoreo y Auditorías:\*\* - Establecer un \*\*sistema de monitoreo continuo\*\* para evaluar el cumplimiento de las normativas y la efectividad de las medidas de seguridad implementadas. - Programar \*\*auditorías internas\*\* periódicas para revisar el cumplimiento y realizar ajustes necesarios.

8. \*\*Colaboración con Proveedores de Servicios:\*\* - Trabajar estrechamente con los proveedores de servicios de pago y tecnología para asegurar que estén alineados con las nuevas regulaciones de VISA. - Evaluar la posibilidad de \*\*contratar consultores\*\* especializados en cumplimiento normativo para obtener asesoría adicional.

9. \*\*Gestión de Riesgos:\*\* - Desarrollar un \*\*plan de gestión de riesgos\*\* que contemple los posibles impactos financieros y reputacionales del incumplimiento. - Realizar análisis de riesgo periódicos para identificar y mitigar vulnerabilidades en los procesos de pago.

10. \*\*Comunicación con Clientes:\*\* - Informar a los clientes sobre las medidas que se están tomando para garantizar la seguridad de sus datos y transacciones. - Establecer canales de comunicación para que los clientes puedan reportar problemas o inquietudes relacionadas con la seguridad.

## Conclusión

La implementación de estas recomendaciones no solo ayudará a los comercios electrónicos y entidades reguladas a cumplir con las nuevas reglas de seguridad de VISA, sino que también fortalecerá la confianza del consumidor y protegerá la reputación del comercio. La proactividad en la adaptación a estas normativas es clave para asegurar un entorno de transacciones seguras y eficientes.

# 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 mencionados:

1. \*\*Visa Core Rules y Visa Product and Service Rules\*\* - Documento que contiene las reglas fundamentales y los servicios ofrecidos por VISA, incluyendo las actualizaciones de seguridad.

2. \*\*Resumen de Cambios (October 2024)\*\* - Documento que detalla los ajustes y requisitos nuevos que impactan a adquirentes, procesadores y emisores.

3. \*\*Visa Online\*\* - Plataforma donde se pueden acceder a las ediciones más recientes de los documentos de VISA, incluyendo las reglas y especificaciones de seguridad.

4. \*\*Visa Secure: Nuevas Extensiones de Mensaje Globales\*\* - Documento que describe las nuevas especificaciones implementadas a partir del 15 de abril del 2025, incluyendo la Visa Additional Data Extension y la Visa Program Data Extension.

Estas referencias son esenciales para proporcionar un contexto completo y permitir a los lectores acceder a la documentación oficial para una comprensión más profunda de las normativas y cambios en las reglas de seguridad de VISA.