**Informe sobre las Nuevas Reglas de Seguridad de VISA para Comercios Electrónicos**

Análisis y Recomendaciones para la Implementación de Normativas de Seguridad en el Comercio Electrónico

26/04/2025

# 1. Executive Summary

* Ejecutivo:\*\*

El informe detalla las actualizaciones de las reglas de seguridad de VISA para comercios electrónicos, efectivas a partir de octubre de 2024. Se han revisado documentos clave, incluyendo las Visa Core Rules y el Visa Merchant Data Standards Manual, disponibles en Visa Online. Entre los cambios más significativos se encuentran nuevos recargos por incumplimiento para comercios de Nivel 3, que entrarán en vigor el 9 de febrero de 2025, y requisitos de presentación de certificados para Miembros Patrocinados, vigentes desde el 12 de enero de 2025. Además, los emisores deberán reportar actividad fraudulenta de inmediato, con sanciones por incumplimiento a partir del 12 de abril de 2025. Se recomienda a los comercios implementar medidas de contención y cumplir con la norma PCI DSS para garantizar un entorno seguro y eficiente.

# 2. Alcance

## Alcance del Informe

El presente informe tiene como propósito proporcionar un análisis exhaustivo de las nuevas reglas de seguridad implementadas por VISA para comercios electrónicos, con un enfoque en las actualizaciones más recientes y su impacto en los diferentes actores del ecosistema de pagos. Este documento está diseñado para ser una guía informativa para comerciantes, procesadores de pagos y emisores, facilitando la comprensión de las normativas vigentes y los cambios que entrarán en vigor en el futuro cercano.

## Límites del Informe

1. \*\*Cobertura Temporal\*\*: El informe se centra en las actualizaciones de octubre de 2024 y las implicaciones de los nuevos recargos que entrarán en vigor el 9 de febrero de 2025. No se abordarán normativas anteriores o cambios que puedan surgir después de esta fecha.

2. \*\*Ámbito Geográfico\*\*: Aunque las reglas de VISA son aplicables a nivel global, este informe se centrará en las implicaciones para comercios electrónicos en regiones específicas donde VISA tiene una presencia significativa. Se recomienda a los lectores considerar las variaciones locales en la implementación de estas reglas.

3. \*\*Actores Involucrados\*\*: El análisis se limita a los comercios electrónicos, procesadores de pagos y emisores de tarjetas. No se incluirán detalles sobre otros actores del ecosistema de pagos, como bancos o instituciones financieras que no estén directamente relacionados con las transacciones electrónicas.

4. \*\*Aspectos Técnicos\*\*: Si bien se proporcionará un resumen de las nuevas reglas y su impacto, el informe no profundizará en aspectos técnicos específicos de implementación o en la infraestructura tecnológica necesaria para cumplir con las nuevas normativas.

5. \*\*Recomendaciones\*\*: El informe no incluirá recomendaciones específicas para la implementación de las nuevas reglas, sino que se limitará a presentar los cambios normativos y sus implicaciones generales.

Este informe busca servir como un recurso clave para que los interesados comprendan las nuevas exigencias de seguridad de VISA y se preparen adecuadamente para su cumplimiento.

# 3. Análisis Regulatorio

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

Este análisis regulatorio se centra en las nuevas reglas de seguridad de VISA, que entrarán en vigor en 2025. Se desglosan los principales requisitos normativos, las obligaciones para las entidades reguladas, los procesos de cumplimiento necesarios y los riesgos asociados con el incumplimiento.

## 1. Principales Requisitos Normativos Identificados

## 1.1 Actualización de Reglas de Seguridad

* \*\*Documentos Clave\*\*: Visa Core Rules, Visa Product and Service Rules y Visa Merchant Data Standards Manual.
* \*\*Fecha de Vigencia\*\*: Actualizaciones disponibles desde octubre de 2024, con cambios específicos que entran en vigor en 2025.

## 1.2 Requisitos de Notificación y Reporte

* \*\*Compromisos de Seguridad\*\*: Nuevos recargos por incumplimiento escalonados para comercios de Nivel 3, vigentes desde el 9 de febrero de 2025.
* \*\*Informes de Actividad de Fraude\*\*: Los emisores deben reportar actividad fraudulenta inmediatamente, con sanciones por incumplimiento a partir del 12 de abril de 2025.

## 1.3 Autenticación y Certificación

* \*\*Actualización de Certificados SSL\*\*: Los clientes deben actualizar sus certificados antes del 1 de junio de 2025 para evitar interrupciones en el servicio.

## 1.4 Vigilancia de Sanciones

* \*\*Revisiones Periódicas\*\*: Obligación de revisar listas de sanciones para evitar la prestación de servicios a individuos o entidades sancionadas.

## 2. Obligaciones para las Entidades Reguladas

## 2.1 Comercios Electrónicos

* \*\*Cumplimiento de PCI DSS\*\*: Mantener la conformidad con el estándar de seguridad de datos de la industria de tarjetas de pago.
* \*\*Planes de Contención\*\*: Desarrollar y mantener planes para la notificación y resolución de actividades sospechosas.

## 2.2 Emisores y Procesadores

* \*\*Informes de Fraude\*\*: Establecer procedimientos para la detección y reporte inmediato de actividad fraudulenta.
* \*\*Capacitación Continua\*\*: Proveer formación a los empleados sobre las nuevas regulaciones y prácticas de seguridad.

## 2.3 Miembros Patrocinados

* \*\*Requisitos de Presentación\*\*: Cumplir con los nuevos requisitos de presentación de informes para operaciones fuera de su región principal, vigentes desde el 12 de enero de 2025.

## 3. Procesos de Cumplimiento Necesarios

## 3.1 Implementación de Medidas de Seguridad

* \*\*Contención de Incidentes\*\*: Establecer protocolos claros para la contención y corrección de incidentes de seguridad.
* \*\*Auditorías Internas\*\*: Realizar auditorías regulares para verificar el cumplimiento de las normas de seguridad.

## 3.2 Actualización de Certificados

* \*\*Proceso de Solicitud\*\*: Asegurar que los certificados SSL sean solicitados y actualizados antes de la fecha límite del 1 de junio de 2025.

## 3.3 Monitoreo de Sanciones

* \*\*Sistema de Vigilancia\*\*: Implementar un sistema para la revisión continua de las listas de sanciones y asegurar que no se presten servicios a entidades prohibidas.

## 4. Riesgos y Consecuencias del Incumplimiento

## 4.1 Sanciones Financieras

* \*\*Recargos por Incumplimiento\*\*: Comercios de Nivel 3 enfrentarán recargos escalonados si no cumplen con las nuevas reglas, lo que podría impactar significativamente su rentabilidad.

## 4.2 Pérdida de Confianza

* \*\*Impacto en la Reputación\*\*: Incidentes de fraude o incumplimiento pueden dañar la reputación de la marca y resultar en la pérdida de clientes.

## 4.3 Consecuencias Legales

* \*\*Acciones Legales\*\*: El incumplimiento de las normativas puede llevar a acciones legales por parte de VISA o de consumidores afectados, resultando en costos adicionales.

## 4.4 Interrupciones en el Servicio

* \*\*Disrupciones Operativas\*\*: La falta de actualización de certificados SSL puede resultar en interrupciones en el servicio, afectando la capacidad de los comercios para procesar pagos.

## Conclusiones

Las nuevas reglas de seguridad de VISA representan un cambio significativo en el ecosistema de pagos electrónicos. Es crucial que todos los actores involucrados comprendan y cumplan con estas regulaciones para evitar sanciones y proteger tanto su reputación como la seguridad de sus clientes. Para más información, se recomienda acceder a los recursos disponibles en el [Visa Support Hub](https://www.visa.com/support) y la documentación completa en Visa Online.

# 4. Conclusiones

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

1. \*\*Urgencia en la Preparación para el Cumplimiento\*\*: La entrada en vigor de las nuevas reglas de seguridad de VISA en 2025 exige que los comercios electrónicos y otros actores del ecosistema de pagos inicien de inmediato la preparación para cumplir con los requisitos establecidos. Esto incluye la actualización de certificados SSL, la implementación de medidas de seguridad adecuadas y la capacitación del personal.

2. \*\*Enfoque en la Prevención del Fraude\*\*: La obligación de reportar actividad fraudulenta de manera inmediata y la implementación de planes de contención son esenciales para mitigar riesgos. Los emisores y procesadores deben establecer procedimientos robustos para la detección y respuesta a incidentes de fraude, lo que no solo protege a los consumidores, sino que también preserva la integridad del sistema de pagos.

3. \*\*Impacto Financiero y Reputacional\*\*: Las sanciones financieras por incumplimiento, especialmente para los comercios de Nivel 3, pueden tener un efecto adverso significativo en la rentabilidad. Además, la pérdida de confianza del consumidor debido a incidentes de seguridad puede resultar en una disminución de la base de clientes y en un daño duradero a la reputación de la marca.

4. \*\*Responsabilidad Compartida\*\*: Todos los actores, incluidos comercios electrónicos, emisores, procesadores y miembros patrocinados, tienen responsabilidades claras en el cumplimiento de las nuevas normativas. La colaboración y la comunicación efectiva entre estas partes son fundamentales para garantizar un enfoque cohesivo hacia la seguridad.

5. \*\*Riesgos Legales y Operativos\*\*: El incumplimiento de las normativas no solo puede resultar en sanciones financieras, sino también en acciones legales que pueden acarrear costos adicionales y complicaciones operativas. Las interrupciones en el servicio debido a la falta de actualización de certificados SSL pueden afectar gravemente la capacidad de los comercios para operar, lo que subraya la importancia de la planificación anticipada.

6. \*\*Vigilancia Continua y Adaptación\*\*: La implementación de un sistema de vigilancia para revisar listas de sanciones y asegurar el cumplimiento continuo es crucial. Las entidades deben estar preparadas para adaptarse a cambios futuros en las regulaciones y en el entorno de amenazas de seguridad.

7. \*\*Recursos y Soporte\*\*: Se recomienda que las entidades reguladas accedan a los recursos disponibles en el Visa Support Hub y en Visa Online para obtener información actualizada y orientación sobre el cumplimiento normativo. La educación continua y la actualización de conocimientos son esenciales para enfrentar los desafíos de seguridad en el comercio electrónico.

En resumen, el cumplimiento de las nuevas reglas de seguridad de VISA no solo es una obligación regulatoria, sino también una estrategia crítica para proteger la integridad del negocio y la confianza del consumidor en un entorno de pagos cada vez más complejo y desafiante.

# 5. Recomendaciones

A continuación, se presentan recomendaciones prácticas y accionables para el cumplimiento de las nuevas reglas de seguridad de VISA, basadas en las conclusiones del análisis normativo:

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

## 1. \*\*Planificación y Preparación Inmediata\*\*

* \*\*Auditoría de Seguridad\*\*: Realizar una auditoría de seguridad integral para identificar vulnerabilidades actuales en los sistemas de pago y en la infraestructura de TI.
* \*\*Actualización de Certificados SSL\*\*: Asegurarse de que todos los certificados SSL estén actualizados y cumplan con los estándares de seguridad requeridos. Implementar un calendario de renovación y monitoreo de certificados.

## 2. \*\*Fortalecimiento de la Prevención del Fraude\*\*

* \*\*Implementación de Tecnología de Detección de Fraude\*\*: Invertir en soluciones de software que utilicen inteligencia artificial y aprendizaje automático para detectar patrones de fraude en tiempo real.
* \*\*Desarrollo de Protocolos de Respuesta\*\*: Establecer y documentar procedimientos claros para la respuesta a incidentes de fraude, incluyendo la notificación inmediata a las partes afectadas y a las autoridades pertinentes.

## 3. \*\*Gestión de Riesgos Financieros y Reputacionales\*\*

* \*\*Evaluación de Impacto Financiero\*\*: Realizar un análisis de costo-beneficio para evaluar el impacto potencial de las sanciones por incumplimiento y la pérdida de confianza del consumidor.
* \*\*Estrategias de Comunicación\*\*: Desarrollar un plan de comunicación para abordar cualquier incidente de seguridad, asegurando que los clientes estén informados y que se tomen medidas para mitigar el daño a la reputación.

## 4. \*\*Colaboración y Responsabilidad Compartida\*\*

* \*\*Establecimiento de Canales de Comunicación\*\*: Crear foros regulares de discusión entre todos los actores involucrados (comercios, emisores, procesadores) para compartir mejores prácticas y actualizaciones sobre cumplimiento.
* \*\*Definición de Roles y Responsabilidades\*\*: Documentar y comunicar claramente las responsabilidades de cada parte en el cumplimiento de las normativas de seguridad.

## 5. \*\*Prevención de Riesgos Legales y Operativos\*\*

* \*\*Revisión Legal\*\*: Consultar con asesores legales para entender las implicaciones de las nuevas normativas y cómo se aplican a la operación del negocio.
* \*\*Plan de Contingencia\*\*: Desarrollar un plan de contingencia que incluya procedimientos para la recuperación ante desastres y la continuidad del negocio en caso de interrupciones operativas.

## 6. \*\*Vigilancia Continua y Adaptación\*\*

* \*\*Monitoreo de Cumplimiento\*\*: Implementar un sistema de monitoreo continuo que revise el cumplimiento de las normativas y ajuste las políticas y procedimientos según sea necesario.
* \*\*Actualización de Políticas de Seguridad\*\*: Revisar y actualizar regularmente las políticas de seguridad para reflejar cambios en las regulaciones y en el entorno de amenazas.

## 7. \*\*Acceso a Recursos y Educación Continua\*\*

* \*\*Capacitación del Personal\*\*: Organizar sesiones de capacitación regulares para el personal sobre las nuevas reglas de seguridad de VISA y las mejores prácticas en ciberseguridad.
* \*\*Utilización de Recursos de VISA\*\*: Acceder a los recursos disponibles en el Visa Support Hub y Visa Online para mantenerse al día con las actualizaciones normativas y recibir orientación sobre el cumplimiento.

## Implementación de un Cronograma de Acción

* \*\*Corto Plazo (0-6 meses)\*\*: Realizar auditorías de seguridad, actualizar certificados SSL y establecer protocolos de respuesta a incidentes.
* \*\*Mediano Plazo (6-12 meses)\*\*: Implementar tecnología de detección de fraude, desarrollar un plan de comunicación y establecer canales de colaboración.
* \*\*Largo Plazo (12-24 meses)\*\*: Monitorear el cumplimiento, actualizar políticas de seguridad y proporcionar capacitación continua al personal.

Al seguir estas recomendaciones, las entidades reguladas podrán no solo cumplir con las nuevas reglas de seguridad de VISA, sino también fortalecer su postura de seguridad general y proteger la confianza del consumidor en un entorno de pagos en constante evolución.

# 6. Referencias

Las principales fuentes, documentos oficiales y normativas mencionadas en el análisis normativo que deberían incluirse en una sección de referencias son:

1. \*\*Visa Core Rules\*\* - Documento que establece las reglas fundamentales para las transacciones y operaciones de VISA. 2. \*\*Visa Product and Service Rules\*\* - Documento que detalla las normas específicas relacionadas con los productos y servicios ofrecidos por VISA. 3. \*\*Visa Merchant Data Standards Manual\*\* - Manual que proporciona directrices sobre los estándares de datos que deben seguir los comerciantes para garantizar la seguridad y la conformidad. 4. \*\*Resumen de Cambios\*\* - Documentación que detalla las actualizaciones y cambios recientes en las reglas de seguridad de VISA, disponible en Visa Online. 5. \*\*What To Do If Compromised\*\* - Documento que explica los procedimientos a seguir en caso de un compromiso de seguridad, incluyendo la implementación de nuevos recargos por incumplimiento.

Estas referencias son esenciales para entender el contexto y los requisitos normativos que afectan a los comercios electrónicos en relación con las nuevas reglas de seguridad de VISA.