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

Un análisis exhaustivo de las recientes actualizaciones en las regulaciones de seguridad para proteger transacciones en línea

27/04/2025

# 1. Executive Summary

* Ejecutivo\*\*

VISA ha introducido nuevas reglas de seguridad para fortalecer la protección en las transacciones de comercio electrónico, enfocándose en la mitigación del fraude y la autenticación de transacciones. Las principales actualizaciones incluyen la implementación de la "Visa Additional Data Extension", que permitirá el intercambio de datos adicionales entre adquirentes y comerciantes, y la "Visa Program Data Extension", que informará sobre el cumplimiento de las transacciones con los programas de autenticación de VISA. La publicación de estas extensiones está programada para el 29 de enero de 2025, con habilitación oficial el 15 de abril de 2025. Además, se establecen requisitos específicos para el llenado de campos en transacciones, lo que es crucial para evitar denegaciones. Estas medidas buscan mejorar la seguridad y la detección temprana de fraudes en el comercio electrónico.

# 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. Se centra en las especificaciones técnicas, los objetivos de seguridad y las implicaciones para los comerciantes y adquirentes en el contexto de las transacciones en línea.

## Límites del Informe

1. \*\*Cobertura Temporal\*\*: El informe se basa en la información disponible hasta octubre de 2023 y considera las actualizaciones más recientes anunciadas por VISA, con fechas de implementación específicas que se extienden hasta 2025.

2. \*\*Ámbito Geográfico\*\*: Aunque las reglas de VISA son aplicables a nivel global, el informe no aborda variaciones regionales o locales en la implementación de estas normas, centrándose en las directrices generales.

3. \*\*Aspectos Técnicos\*\*: Se detallan las especificaciones técnicas relacionadas con la Visa Additional Data Extension y otros métodos de autenticación, pero no se incluye un análisis profundo de las tecnologías subyacentes o de los sistemas de pago específicos utilizados por los comerciantes.

4. \*\*Perspectivas de Cumplimiento\*\*: El informe no proporciona asesoramiento legal ni recomendaciones sobre cómo cumplir con las nuevas reglas, sino que se limita a describir las normativas y su propósito.

5. \*\*Impacto Económico\*\*: No se evalúa el impacto económico de estas nuevas reglas en el sector del comercio electrónico, ni se analizan las posibles reacciones del mercado o de los consumidores.

Este informe está diseñado para ser una herramienta informativa para comerciantes, adquirentes y otros interesados en el ámbito de la seguridad de pagos electrónicos, facilitando una comprensión clara de las nuevas normativas de VISA y su relevancia en el entorno actual de 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 Extensiones de Mensaje

## - \*\*Visa Additional Data Extension\*\*

* \*\*Requisito\*\*: Los comerciantes tienen la opción de compartir datos adicionales, pero deben incluir el Número de Orden de Compra para participar en el programa CE3.0.
* \*\*Fecha de Implementación\*\*: Publicación el 29 de enero de 2025 y habilitación el 15 de abril de 2025.

## - \*\*Visa Program Data Extension\*\*

* \*\*Requisito\*\*: Los comerciantes y adquirentes deben estar informados sobre la conformidad de las transacciones con los programas de autenticación de VISA.
* \*\*Generación\*\*: Esta extensión será generada automáticamente por el Servidor de Directorio de Visa Secure.

## 1.2 Gestión de Datos

* \*\*Requisitos de Llenado\*\*: Desde el 11 de julio de 2025, los adquirentes, emisores y comerciantes deben completar campos específicos en transacciones AFT y OCT para evitar denegaciones.

## 1.3 Control de Sanciones

* \*\*Verificación de Sanciones\*\*: Los miembros de VISA deben verificar periódicamente que sus clientes no estén en listas de sanciones aplicables, tomando medidas si se detectan coincidencias.

## 2. Obligaciones para las Entidades Reguladas

## 2.1 Comerciantes

* \*\*Cumplimiento de Nuevas Especificaciones\*\*: Deben adaptarse a las nuevas extensiones de mensaje y cumplir con los requisitos de llenado para transacciones.
* \*\*Participación en Programas de Autenticación\*\*: Deben estar informados sobre la conformidad de sus transacciones con los programas de VISA.

## 2.2 Adquirentes y Emisores

* \*\*Implementación de Cambios\*\*: Deben asegurarse de que sus sistemas estén actualizados para manejar las nuevas extensiones de mensaje y cumplir con los requisitos de llenado.
* \*\*Verificación de Sanciones\*\*: Deben establecer procedimientos para verificar que sus clientes no estén sujetos a sanciones.

## 2.3 Miembros de VISA

* \*\*Responsabilidad de Cumplimiento\*\*: Cada miembro debe asegurarse de que sus operaciones cumplan con las nuevas reglas y regulaciones establecidas por VISA.

## 3. Procesos de Cumplimiento Necesarios

## 3.1 Actualización de Sistemas

* \*\*Adaptación Tecnológica\*\*: Los comerciantes y adquirentes deben actualizar sus sistemas de procesamiento de pagos para integrar las nuevas extensiones de mensaje antes de las fechas de habilitación.

## 3.2 Capacitación del Personal

* \*\*Formación\*\*: Es fundamental que el personal de los comercios y adquirentes reciba capacitación sobre las nuevas reglas y procedimientos de cumplimiento.

## 3.3 Verificación de Sanciones

* \*\*Implementación de Procedimientos\*\*: Los miembros de VISA deben establecer un proceso regular para verificar las listas de sanciones y documentar las acciones tomadas en caso de coincidencias.

## 3.4 Documentación y Recursos

* \*\*Acceso a Recursos\*\*: Los comercios deben utilizar la documentación y recursos actualizados proporcionados por VISA para garantizar el cumplimiento.

## 4. Riesgos y Consecuencias del Incumplimiento

## 4.1 Riesgos Financieros

* \*\*Multas y Sanciones\*\*: El incumplimiento de las nuevas reglas puede resultar en multas significativas y sanciones impuestas por VISA, lo que podría afectar la viabilidad financiera del comercio.

## 4.2 Pérdida de Confianza del Cliente

* \*\*Impacto en la Reputación\*\*: Las violaciones de seguridad pueden llevar a la pérdida de confianza por parte de los consumidores, lo que podría traducirse en una disminución de las ventas y la lealtad del cliente.

## 4.3 Riesgo de Fraude

* \*\*Aumento de Fraude\*\*: La falta de cumplimiento con las nuevas medidas de seguridad puede resultar en un aumento de intentos de fraude, lo que podría comprometer la seguridad del ecosistema de pagos.

## 4.4 Consecuencias Legales

* \*\*Acciones Legales\*\*: El incumplimiento puede dar lugar a acciones legales por parte de consumidores o entidades reguladoras, lo que podría resultar en costos adicionales y daños a la reputación.

## 5. Conclusión

Las nuevas reglas de seguridad de VISA representan un esfuerzo significativo para fortalecer la protección en las transacciones de comercio electrónico. Es imperativo que todos los actores del ecosistema de pagos se adapten a estas regulaciones para mitigar riesgos y asegurar la integridad de sus operaciones. La implementación efectiva de estas reglas no solo es un requisito normativo, sino también una estrategia esencial para mantener la confianza del consumidor y la estabilidad del mercado.

# 4. Conclusiones

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

1. \*\*Adaptación Obligatoria y Oportuna\*\*: La implementación de las nuevas reglas de seguridad de VISA es un proceso que requiere una adaptación tecnológica y organizativa significativa por parte de comerciantes, adquirentes y emisores. La fecha límite para la habilitación de las nuevas extensiones de mensaje y los requisitos de llenado es crítica, y el incumplimiento puede resultar en consecuencias financieras severas. Por lo tanto, es esencial que las entidades comiencen a realizar las actualizaciones necesarias de sus sistemas y procesos de inmediato.

2. \*\*Capacitación y Conciencia del Personal\*\*: La formación del personal es un aspecto fundamental para garantizar el cumplimiento normativo. La falta de conocimiento sobre las nuevas regulaciones puede llevar a errores en la gestión de transacciones y a un incumplimiento involuntario. Las entidades deben invertir en programas de capacitación que aseguren que todos los empleados comprendan las nuevas reglas y su importancia en la seguridad de las transacciones.

3. \*\*Verificación de Sanciones como Prioridad\*\*: La obligación de verificar que los clientes no estén en listas de sanciones es un componente crítico de las nuevas regulaciones. Las entidades deben establecer procedimientos robustos para realizar estas verificaciones de manera regular y documentar las acciones tomadas. Esto no solo es un requisito normativo, sino que también ayuda a mitigar riesgos legales y financieros.

4. \*\*Riesgos Asociados al Incumplimiento\*\*: El incumplimiento de las nuevas reglas puede acarrear riesgos financieros significativos, incluyendo multas y sanciones, así como un impacto negativo en la reputación de la marca. La pérdida de confianza del consumidor puede resultar en una disminución de las ventas y la lealtad, lo que subraya la importancia de cumplir con las regulaciones no solo como un requisito legal, sino como una estrategia comercial.

5. \*\*Fortalecimiento de la Seguridad en el Ecosistema de Pagos\*\*: Las nuevas reglas de seguridad de VISA son un paso importante hacia la mejora de la seguridad en el comercio electrónico. La implementación efectiva de estas regulaciones no solo protegerá a los comerciantes y consumidores, sino que también contribuirá a la estabilidad del ecosistema de pagos en su conjunto. La colaboración entre todos los actores del sector es esencial para crear un entorno más seguro y confiable.

6. \*\*Documentación y Recursos\*\*: Es crucial que los comerciantes y adquirentes accedan y utilicen la documentación y recursos proporcionados por VISA para garantizar el cumplimiento. La falta de acceso a información actualizada puede resultar en malentendidos y errores en la implementación de las nuevas reglas.

7. \*\*Implicaciones a Largo Plazo\*\*: A medida que el comercio electrónico continúa creciendo, las regulaciones de seguridad como las de VISA se volverán cada vez más relevantes. Las entidades que no se adapten a estas normativas corren el riesgo de quedar rezagadas en un mercado competitivo, donde la seguridad y la confianza del consumidor son primordiales.

En resumen, la adaptación a las nuevas reglas de seguridad de VISA es un imperativo estratégico que va más allá del cumplimiento normativo. Las entidades deben ver estas regulaciones como una oportunidad para fortalecer su posición en el mercado y mejorar la confianza del consumidor en sus operaciones.

# 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 las conclusiones del análisis normativo:

## Recomendaciones Prácticas para el Cumplimiento Normativo

## 1. \*\*Plan de Implementación Inmediato\*\*

* \*\*Establecer un cronograma\*\*: Desarrollar un plan de acción con fechas límite claras para la actualización de sistemas y procesos. Incluir hitos para la revisión y prueba de las nuevas extensiones de mensaje.
* \*\*Asignar responsabilidades\*\*: Designar un equipo responsable de la implementación que incluya representantes de TI, operaciones y cumplimiento normativo.

## 2. \*\*Programa de Capacitación Integral\*\*

* \*\*Desarrollar módulos de capacitación\*\*: Crear programas de formación específicos sobre las nuevas reglas de seguridad de VISA, adaptados a diferentes niveles de personal (ejecutivos, operativos, técnicos).
* \*\*Realizar sesiones de actualización periódicas\*\*: Programar capacitaciones regulares para mantener al personal informado sobre cambios en las regulaciones y mejores prácticas en seguridad.

## 3. \*\*Procedimientos de Verificación de Sanciones\*\*

* \*\*Implementar un sistema automatizado\*\*: Utilizar software que realice verificaciones automáticas de listas de sanciones y que genere informes de cumplimiento.
* \*\*Documentar procesos\*\*: Establecer un protocolo claro para la verificación de sanciones, incluyendo la documentación de las acciones realizadas y los resultados obtenidos.

## 4. \*\*Evaluación de Riesgos y Plan de Mitigación\*\*

* \*\*Realizar un análisis de riesgos\*\*: Identificar y evaluar los riesgos asociados al incumplimiento de las nuevas reglas, así como sus posibles consecuencias financieras y reputacionales.
* \*\*Desarrollar un plan de mitigación\*\*: Crear estrategias para abordar y reducir los riesgos identificados, incluyendo la asignación de recursos para la gestión de incidentes.

## 5. \*\*Fortalecimiento de la Seguridad Cibernética\*\*

* \*\*Auditorías de seguridad regulares\*\*: Realizar evaluaciones periódicas de la infraestructura de seguridad para identificar vulnerabilidades y asegurar que se cumplan las nuevas normas.
* \*\*Implementar medidas de seguridad adicionales\*\*: Considerar la adopción de tecnologías como la autenticación multifactor (MFA) y la encriptación de datos para proteger la información del cliente.

## 6. \*\*Acceso a Documentación y Recursos de VISA\*\*

* \*\*Crear un repositorio de recursos\*\*: Establecer un sistema de gestión de documentos donde se centralicen todos los recursos y guías proporcionadas por VISA.
* \*\*Suscribirse a actualizaciones\*\*: Mantenerse al día con las comunicaciones de VISA y otras entidades relevantes para recibir notificaciones sobre cambios normativos y mejores prácticas.

## 7. \*\*Monitoreo y Revisión Continua\*\*

* \*\*Establecer indicadores de rendimiento\*\*: Definir métricas para evaluar el cumplimiento normativo y la efectividad de las medidas implementadas.
* \*\*Revisiones periódicas\*\*: Programar revisiones regulares del cumplimiento normativo y de la efectividad de las políticas y procedimientos establecidos, ajustando según sea necesario.

## 8. \*\*Colaboración con Actores del Sector\*\*

* \*\*Participar en foros y grupos de trabajo\*\*: Unirse a asociaciones del sector y participar en foros de discusión sobre cumplimiento normativo y seguridad en el comercio electrónico.
* \*\*Compartir mejores prácticas\*\*: Colaborar con otros comerciantes y adquirentes para intercambiar experiencias y estrategias exitosas en la implementación de las nuevas reglas.

## Conclusión

La implementación de estas recomendaciones no solo ayudará a cumplir con las nuevas reglas de seguridad de VISA, sino que también fortalecerá la posición competitiva de las entidades en el mercado, mejorando la confianza del consumidor y la seguridad en el ecosistema de pagos.

# 6. Referencias

Para incluir en una sección de referencias del informe sobre las Nuevas Reglas de Seguridad de VISA para Comercios Electrónicos, se pueden considerar las siguientes fuentes y documentos oficiales relevantes:

## 1. \*\*Documentación de VISA\*\*

* "VISA Security Standards" - Documento que detalla las normas de seguridad que VISA establece para proteger las transacciones electrónicas.
* "VISA Additional Data Extension Specification" - Documento específico que describe la extensión de datos adicionales y su implementación.

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

* "VISA Evidence of Compliance 3.0" - Documento que explica los requisitos y procedimientos para la evidencia de cumplimiento en transacciones.

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

* "VISA Intelligent Data Exchange Guidelines" - Documento que proporciona directrices sobre el intercambio de datos inteligentes y su aplicación en transacciones.

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

* "PCI Data Security Standard" - Normativa que establece los requisitos de seguridad para proteger la información de tarjetas de pago.

## 5. \*\*Regulaciones de Protección de Datos\*\*

* "Reglamento General de Protección de Datos (GDPR)" - Normativa de la Unión Europea que regula el tratamiento de datos personales y su protección.

## 6. \*\*Publicaciones de la Asociación de Comercio Electrónico\*\*

* "Best Practices for E-Commerce Security" - Documento que ofrece recomendaciones sobre las mejores prácticas para la seguridad en el comercio electrónico.

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

* Comunicados oficiales que anuncian la implementación de nuevas reglas y especificaciones de seguridad.

Estas referencias proporcionarán un contexto sólido y una base normativa para el análisis presentado en el informe.