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

A partir del 15 de abril de 2025, VISA implementará dos nuevas extensiones de mensaje globales para mejorar la seguridad en comercios electrónicos: la \*\*Visa Additional Data Extension\*\* y la \*\*Visa Program Data Extension\*\*. La primera permitirá el intercambio de datos adicionales, siendo obligatorio incluir el \*\*Número de Orden de Compra\*\* para participar en programas como Compelling Evidence 3.0. La segunda extensión proporcionará a adquirentes y comercios información sobre el cumplimiento de sus transacciones con los programas de autenticación de VISA. Las fechas clave incluyen la publicación de nuevas especificaciones el 29 de enero de 2025 y la guía Visa Secure el 15 de febrero de 2025. Estas medidas buscan fortalecer la protección contra el fraude y mejorar la seguridad en las transacciones electrónicas.

# 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 los comercios electrónicos, con un enfoque particular en las especificaciones y extensiones de mensaje que entrarán en vigor a partir del 15 de abril de 2025.

## Objetivos del Informe

1. \*\*Informar sobre las Nuevas Especificaciones\*\*: Describir las nuevas extensiones de mensaje globales, incluyendo la Visa Additional Data Extension y la Visa Program Data Extension, y su impacto en la seguridad de las transacciones electrónicas. 2. \*\*Analizar el Cumplimiento\*\*: Evaluar cómo estas nuevas reglas afectarán el cumplimiento normativo de los comercios y adquirentes en relación con los programas de autenticación de VISA. 3. \*\*Proporcionar Recomendaciones\*\*: Sugerir mejores prácticas para la implementación de estas nuevas reglas y cómo los comercios pueden adaptarse a los cambios requeridos.

## Límites del Informe

* \*\*Temporalidad\*\*: Este informe se centra exclusivamente en las reglas que entrarán en vigor a partir del 15 de abril de 2025, sin abordar normativas anteriores o futuras que no estén directamente relacionadas con este cambio.
* \*\*Ámbito Geográfico\*\*: El análisis se limita a las regulaciones aplicables en los mercados donde VISA opera, sin considerar variaciones locales o regionales que puedan existir en otros contextos.
* \*\*Enfoque Técnico\*\*: El informe se centrará en aspectos técnicos y normativos de las nuevas reglas, sin entrar en detalles sobre la implementación específica en sistemas de pago o plataformas de comercio electrónico.

Este alcance busca asegurar que el informe sea una herramienta útil y relevante para los interesados en la seguridad de las transacciones electrónicas y el cumplimiento normativo en el contexto de las nuevas regulaciones de VISA.

# 3. Análisis Regulatorio

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

## 1. Principales Requisitos Normativos Identificados

Las nuevas reglas de seguridad de VISA introducen dos extensiones de mensaje globales que son fundamentales para la seguridad de las transacciones de comercio electrónico:

## 1.1 Visa Additional Data Extension

* \*\*Objetivo\*\*: Mejorar la seguridad de las transacciones y proteger a los comercios contra el fraude.

## - \*\*Requisitos Específicos\*\*

* Inclusión obligatoria del \*\*Número de Orden de Compra\*\* para participar en programas como Compelling Evidence 3.0.
* Envío y recepción de datos adicionales que fortalezcan la autenticación y validación de las transacciones.

## 1.2 Visa Program Data Extension

* \*\*Objetivo\*\*: Proporcionar información sobre el cumplimiento de las transacciones con los programas de autenticación de VISA.

## - \*\*Requisitos Específicos\*\*

* Información sobre el cumplimiento será enviada desde el Servidor de Directorio de VISA en el mensaje de Respuesta de Autenticación.

## 2. Obligaciones para las Entidades Reguladas

Las entidades reguladas, que incluyen comercios y adquirentes, tienen varias obligaciones bajo estas nuevas reglas:

## 2.1 Comercios

* \*\*Implementación de Nuevas Especificaciones\*\*: Deben adaptar sus sistemas para enviar y recibir los nuevos elementos de datos establecidos por las extensiones.
* \*\*Cumplimiento de Requisitos de Datos\*\*: Asegurarse de que el \*\*Número de Orden de Compra\*\* esté presente en todas las transacciones que participen en programas de autenticación.

## 2.2 Adquirentes

* \*\*Facilitación de la Implementación\*\*: Deben trabajar con los comercios para garantizar que se cumplan los nuevos requisitos de seguridad.
* \*\*Monitoreo de Cumplimiento\*\*: Establecer mecanismos para verificar que las transacciones de los comercios cumplen con los programas de autenticación de VISA.

## 3. Procesos de Cumplimiento Necesarios

Para cumplir con las nuevas regulaciones, las entidades reguladas deben seguir varios procesos:

## 3.1 Evaluación de Sistemas

* \*\*Auditoría de Infraestructura\*\*: Realizar una revisión exhaustiva de los sistemas actuales para identificar las modificaciones necesarias para integrar las nuevas extensiones de mensaje.

## 3.2 Capacitación y Concienciación

* \*\*Formación del Personal\*\*: Capacitar a los empleados sobre los nuevos requisitos y la importancia de la seguridad en las transacciones electrónicas.

## 3.3 Implementación Técnica

* \*\*Desarrollo de Software\*\*: Actualizar o desarrollar software que permita la inclusión del \*\*Número de Orden de Compra\*\* y la gestión de los nuevos datos de autenticación.
* \*\*Pruebas de Sistema\*\*: Realizar pruebas exhaustivas para asegurar que los sistemas cumplen con las especificaciones de VISA antes de las fechas de implementación.

## 3.4 Monitoreo Continuo

* \*\*Revisión de Cumplimiento\*\*: Establecer un proceso de revisión continua para asegurar que las transacciones sigan cumpliendo con los nuevos requisitos de seguridad.

## 4. Riesgos y Consecuencias del Incumplimiento

El incumplimiento de las nuevas reglas de VISA puede acarrear serias consecuencias para los comercios y adquirentes:

## 4.1 Riesgos Financieros

* \*\*Multas y Penalizaciones\*\*: VISA puede imponer sanciones económicas a los comercios y adquirentes que no cumplan con las nuevas regulaciones.

## 4.2 Pérdida de Confianza

* \*\*Impacto en la Reputación\*\*: Un incumplimiento puede dañar la reputación de un comercio, afectando la confianza de los consumidores y la relación con los adquirentes.

## 4.3 Riesgos de Seguridad

* \*\*Incremento del Fraude\*\*: La falta de cumplimiento puede resultar en un aumento de las transacciones fraudulentas, lo que podría llevar a pérdidas significativas.

## 4.4 Consecuencias Legales

* \*\*Litigios\*\*: Los comercios que no implementen las medidas adecuadas pueden enfrentar acciones legales por parte de consumidores o entidades financieras afectadas por el fraude.

## Conclusiones

Las nuevas reglas de seguridad de VISA para comercios electrónicos representan un paso significativo hacia la mejora de la seguridad en las transacciones en línea. Es crucial que los comercios y adquirentes comiencen a prepararse para la implementación de estas especificaciones, cumpliendo con los requisitos obligatorios y estableciendo procesos de cumplimiento robustos. La falta de cumplimiento no solo puede resultar en sanciones financieras, sino también en un daño irreparable a la reputación y la confianza del consumidor. Se recomienda a las entidades reguladas mantenerse informadas sobre las actualizaciones y consultar los documentos oficiales de VISA para asegurar una correcta implementación.

# 4. Conclusiones

## Conclusiones Clave sobre la Normativa de Seguridad de VISA para Comercios Electrónicos

1. \*\*Fortalecimiento de la Seguridad en Transacciones\*\*: Las nuevas reglas de VISA introducen medidas significativas para mejorar la seguridad de las transacciones electrónicas, lo que es esencial en un entorno donde el fraude en línea está en aumento. La inclusión obligatoria del \*\*Número de Orden de Compra\*\* y la implementación de las extensiones de mensaje globales son pasos críticos para proteger tanto a los comercios como a los consumidores.

2. \*\*Obligaciones Claras para Comercios y Adquirentes\*\*: Las entidades reguladas deben adaptarse rápidamente a los nuevos requisitos. Esto implica no solo la implementación técnica de los sistemas, sino también la capacitación del personal y el establecimiento de procesos de monitoreo continuo. La colaboración entre comercios y adquirentes es fundamental para garantizar el cumplimiento efectivo de las nuevas normas.

3. \*\*Riesgos Asociados al Incumplimiento\*\*: Las consecuencias del incumplimiento son severas, incluyendo multas, daños a la reputación y un aumento en el riesgo de fraude. Estos riesgos no solo afectan a los comercios individuales, sino que pueden tener repercusiones en toda la red de pagos, afectando la confianza del consumidor en el comercio electrónico en general.

4. \*\*Importancia de la Capacitación y Concienciación\*\*: La formación del personal es un aspecto crítico que no debe ser subestimado. La concienciación sobre la importancia de la seguridad en las transacciones y el cumplimiento de las nuevas regulaciones es esencial para prevenir errores que puedan resultar en incumplimientos.

5. \*\*Necesidad de Monitoreo y Evaluación Continua\*\*: La implementación de un proceso de revisión continua es vital para asegurar que las transacciones se mantengan dentro de los estándares de seguridad establecidos por VISA. Esto no solo ayuda a identificar y corregir problemas de cumplimiento, sino que también permite a los comercios adaptarse a futuras actualizaciones normativas.

6. \*\*Recomendaciones para la Implementación\*\*: Se aconseja a las entidades reguladas que realicen auditorías exhaustivas de sus sistemas actuales, desarrollen software adecuado y realicen pruebas antes de la implementación. Además, mantenerse informados sobre las actualizaciones de VISA y consultar la documentación oficial es crucial para asegurar una transición fluida y efectiva hacia el cumplimiento.

7. \*\*Impacto en la Relación con los Consumidores\*\*: La implementación efectiva de estas normas no solo protege a los comercios de sanciones, sino que también puede fortalecer la confianza del consumidor. Un compromiso visible con la seguridad puede ser un diferenciador clave en un mercado competitivo, mejorando la percepción de la marca y fomentando la lealtad del cliente.

En resumen, la adaptación a las nuevas reglas de seguridad de VISA es un imperativo estratégico para los comercios electrónicos y sus adquirentes. La proactividad en la implementación y el cumplimiento de estas normativas no solo mitigará riesgos financieros y legales, sino que también contribuirá a un ecosistema de comercio electrónico más seguro y confiable.

# 5. Recomendaciones

A continuación, se presentan recomendaciones prácticas y accionables para el cumplimiento de la normativa de seguridad de VISA para comercios electrónicos, basadas en las conclusiones clave del análisis normativo:

## Recomendaciones Prácticas para el Cumplimiento de la Normativa de Seguridad de VISA

## 1. \*\*Implementación Técnica de Nuevas Reglas\*\*

* \*\*Integración del Número de Orden de Compra\*\*: Asegúrese de que todos los sistemas de pago integren el Número de Orden de Compra en las transacciones. Realice pruebas exhaustivas para verificar que esta información se envía correctamente en cada transacción.
* \*\*Adopción de Extensiones de Mensaje Globales\*\*: Actualice los sistemas de procesamiento de pagos para incluir las extensiones de mensaje globales requeridas. Esto puede implicar la colaboración con proveedores de software y adquirentes para garantizar la compatibilidad.

## 2. \*\*Capacitación del Personal\*\*

* \*\*Programas de Formación\*\*: Desarrolle un programa de capacitación regular para todos los empleados involucrados en el procesamiento de pagos y la gestión de la seguridad. Incluya módulos sobre las nuevas regulaciones de VISA, la importancia de la seguridad en las transacciones y cómo identificar posibles fraudes.
* \*\*Simulaciones de Incidentes\*\*: Realice simulaciones de incidentes de seguridad para preparar al personal sobre cómo responder ante posibles brechas de seguridad o fraudes.

## 3. \*\*Establecimiento de Procesos de Monitoreo\*\*

* \*\*Monitoreo Continuo\*\*: Implemente herramientas de monitoreo que analicen las transacciones en tiempo real para detectar patrones inusuales o comportamientos sospechosos. Esto puede incluir la utilización de inteligencia artificial y análisis de datos.
* \*\*Auditorías Regulares\*\*: Programe auditorías internas periódicas para evaluar el cumplimiento de las nuevas normas y la efectividad de las medidas de seguridad implementadas.

## 4. \*\*Gestión de Riesgos y Cumplimiento\*\*

* \*\*Evaluación de Riesgos\*\*: Realice una evaluación de riesgos para identificar áreas vulnerables dentro de su sistema de pagos y desarrolle un plan de mitigación para abordar estos riesgos.
* \*\*Documentación de Cumplimiento\*\*: Mantenga registros detallados de todas las acciones tomadas para cumplir con las normativas de VISA, incluyendo auditorías, capacitaciones y actualizaciones de sistemas.

## 5. \*\*Comunicación con Adquirentes y Proveedores\*\*

* \*\*Colaboración Activa\*\*: Establezca una comunicación fluida con los adquirentes y proveedores de servicios de pago para asegurarse de que están al tanto de las nuevas regulaciones y que sus sistemas están alineados con los requisitos de VISA.
* \*\*Revisiones de Contratos\*\*: Revise los contratos con los adquirentes para asegurarse de que incluyan cláusulas que aborden el cumplimiento de las nuevas normas de seguridad.

## 6. \*\*Actualización de Políticas de Seguridad\*\*

* \*\*Revisión de Políticas Internas\*\*: Actualice las políticas de seguridad y privacidad de la empresa para reflejar las nuevas regulaciones. Asegúrese de que todos los empleados tengan acceso a estas políticas y comprendan su importancia.
* \*\*Plan de Respuesta a Incidentes\*\*: Desarrolle o actualice un plan de respuesta a incidentes que detalle los pasos a seguir en caso de una brecha de seguridad, incluyendo la notificación a las partes afectadas y a las autoridades pertinentes.

## 7. \*\*Fomento de la Confianza del Consumidor\*\*

* \*\*Comunicación Transparente\*\*: Informe a los consumidores sobre las medidas de seguridad implementadas para proteger sus datos y transacciones. Esto puede incluir la publicación de políticas de seguridad en el sitio web y el uso de sellos de confianza.
* \*\*Feedback del Cliente\*\*: Establezca canales para recibir retroalimentación de los consumidores sobre su experiencia de compra y la percepción de seguridad, y utilice esta información para realizar mejoras continuas.

## Conclusión

La implementación de estas recomendaciones no solo ayudará a los comercios electrónicos a cumplir con las normativas de seguridad de VISA, sino que también contribuirá a crear un entorno de comercio electrónico más seguro y confiable, fortaleciendo la relación con los consumidores y minimizando riesgos financieros y legales.

# 6. Referencias

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

1. \*\*VISA Global Security Standards\*\*: Documentación oficial que detalla los estándares de seguridad que VISA establece para los comercios electrónicos y las transacciones.

2. \*\*VISA Secure Program Documentation\*\*: Información específica sobre el programa VISA Secure, que incluye detalles sobre la Evidencia Convincente 3.0 y el Intercambio de Datos Inteligentes.

3. \*\*PCI DSS (Payment Card Industry Data Security Standard)\*\*: Normativa que establece requisitos de seguridad para las organizaciones que manejan información de tarjetas de crédito, relevante para el cumplimiento de las nuevas reglas.

4. \*\*VISA Merchant Guidelines\*\*: Directrices para comercios que operan con VISA, que pueden incluir información sobre la implementación de nuevas extensiones de mensaje.

5. \*\*Comunicados de Prensa de VISA\*\*: Anuncios oficiales que pueden contener información sobre la implementación de nuevas especificaciones y extensiones de seguridad.

6. \*\*Documentación técnica de VISA\*\*: Manuales y guías técnicas que describen cómo implementar las nuevas extensiones de mensaje y asegurar las transacciones electrónicas.

7. \*\*Normativas locales e internacionales sobre comercio electrónico\*\*: Cualquier legislación relevante que pueda influir en la implementación de las nuevas reglas de seguridad, como la GDPR en Europa o la Ley de Protección al Consumidor en otros países.

Incluir estas referencias proporcionará un contexto sólido y una base normativa para el análisis presentado en el informe.