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

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

26/04/2025

# 1. Executive Summary

* Ejecutivo: Nuevas Reglas de Seguridad de VISA para Comercios Electrónicos\*\*

El 29 de enero de 2025, VISA publicará nuevas especificaciones bajo el programa Visa Secure, que incluirán la Visa Additional Data Extension y la Visa Program Data Extension, con el objetivo de fortalecer la seguridad en las transacciones de comercio electrónico y reducir el fraude. Estas extensiones permitirán a los comercios y adquirentes compartir información relevante sobre la conformidad de las transacciones con los programas de autenticación de VISA. Se requerirán acciones proactivas por parte de los adquirentes y proveedores de Servidores 3-D Secure (3DSS) para implementar estas medidas, aunque el intercambio de ciertos datos será opcional. Todos los comercios que utilizan Visa Secure, incluidos los que implementan EMV® 3DS, deberán adaptarse a estos nuevos requisitos para garantizar la seguridad y la integridad de sus operaciones. La habilitación global de estas especificaciones está programada para el 15 de abril de 2025.

# 2. Alcance

## Alcance del Informe

El presente informe tiene como propósito proporcionar un análisis exhaustivo de las nuevas reglas de seguridad de VISA para comercios electrónicos, específicamente en el contexto de la implementación de Visa Secure y sus extensiones de mensaje globales. Este documento se basa en la documentación más reciente y oficial emitida por VISA, con el objetivo de informar a los comerciantes, adquirentes y proveedores de servicios de pago sobre los cambios normativos y las implicaciones que estos tienen en la seguridad de las transacciones electrónicas.

## Límites del Informe

1. \*\*Temporalidad\*\*: El informe se centra en las especificaciones publicadas el 29 de enero de 2025 y su habilitación a nivel mundial el 15 de abril de 2025. No se abordarán cambios anteriores o posteriores a estas fechas.

2. \*\*Contenido\*\*: Se analizarán únicamente las nuevas extensiones de mensaje globales introducidas por VISA, incluyendo la Visa Additional Data Extension y la Visa Program Data Extension. No se incluirán otros aspectos de la normativa de VISA que no estén directamente relacionados con estas extensiones.

3. \*\*Audiencia\*\*: Este informe está dirigido a comerciantes electrónicos, adquirentes, proveedores de servicios de pago y otros actores relevantes en el ecosistema de pagos digitales. No se contempla un análisis para consumidores finales o usuarios individuales de tarjetas.

4. \*\*Enfoque\*\*: El informe se centrará en los objetivos de seguridad y las implicaciones operativas de las nuevas reglas, sin entrar en detalles técnicos profundos que puedan ser más relevantes para desarrolladores o ingenieros de sistemas.

5. \*\*Exclusiones\*\*: No se abordarán las normativas de seguridad de otras entidades o estándares de la industria, como PCI DSS, a menos que se mencionen en relación con las nuevas reglas de VISA.

Este alcance define claramente el propósito y los límites del informe, asegurando que los lectores comprendan el contexto y la relevancia de la información presentada.

# 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 se implementarán a partir de 2025. A continuación, se desglosan los principales requisitos normativos, las obligaciones para las entidades reguladas, los procesos de cumplimiento necesarios y los riesgos asociados al incumplimiento.

## 1. Principales Requisitos Normativos Identificados

## 1.1. Extensiones de Mensaje Globales

* \*\*Visa Additional Data Extension\*\*: Permite la inclusión de datos adicionales en las transacciones, facilitando la implementación de programas de seguridad como CE 3.0 e IDX.
* \*\*Visa Program Data Extension\*\*: Obliga a los comercios y adquirentes a notificar sobre la conformidad de las transacciones con los programas de autenticación de VISA.

## 1.2. Participación en CE 3.0

* \*\*Número de Orden de Compra\*\*: Se establece como un requisito obligatorio para participar en el programa de Evidencia Convincente 3.0, lo que implica que todos los comercios deben asegurarse de incluir este dato en sus transacciones.

## 1.3. Fechas Clave de Implementación

* \*\*Publicación de Especificaciones\*\*: 29 de enero de 2025.
* \*\*Habilitación Global\*\*: 15 de abril de 2025.

## 2. Obligaciones para las Entidades Reguladas

## 2.1. Comercios

* \*\*Implementación de Nuevas Extensiones\*\*: Los comercios deben adaptar sus sistemas para soportar las nuevas extensiones de mensaje, asegurando que puedan manejar los datos adicionales requeridos.
* \*\*Participación en CE 3.0\*\*: Deben garantizar que el número de orden de compra se incluya en todas las transacciones para poder participar en el programa CE 3.0.

## 2.2. Adquirentes y Procesadores de Pagos

* \*\*Actualización de Sistemas\*\*: Los adquirentes deben actualizar sus sistemas y procesos para cumplir con las nuevas especificaciones de VISA, lo que puede incluir la capacitación del personal y la modificación de software.
* \*\*Monitoreo de Conformidad\*\*: Deben establecer mecanismos para monitorear y asegurar que los comercios cumplan con los nuevos requisitos.

## 2.3. Proveedores de Servidores 3-D Secure (3DSS)

* \*\*Facilitación de la Implementación\*\*: Los proveedores de 3DSS deben ofrecer soporte técnico y actualizaciones para que los comercios puedan integrar las nuevas extensiones de manera efectiva.

## 3. Procesos de Cumplimiento Necesarios

## 3.1. Evaluación de Sistemas

* \*\*Auditoría Interna\*\*: Realizar auditorías internas para evaluar la capacidad de los sistemas actuales para manejar las nuevas extensiones de mensaje.
* \*\*Pruebas de Conformidad\*\*: Implementar pruebas de conformidad para asegurar que todos los sistemas estén alineados con las nuevas especificaciones de VISA.

## 3.2. Capacitación y Concienciación

* \*\*Formación del Personal\*\*: Desarrollar programas de capacitación para el personal involucrado en la gestión de transacciones electrónicas, asegurando que comprendan los nuevos requisitos y su importancia.

## 3.3. Documentación y Reporte

* \*\*Registro de Transacciones\*\*: Mantener registros precisos de las transacciones que incluyan el número de orden de compra y otros datos relevantes para facilitar auditorías y revisiones.

## 4. Riesgos y Consecuencias del Incumplimiento

## 4.1. Riesgos Financieros

* \*\*Multas y Sanciones\*\*: El incumplimiento de las nuevas reglas puede resultar en multas significativas impuestas por VISA, así como sanciones adicionales por parte de reguladores financieros.

## 4.2. Pérdida de Confianza del Cliente

* \*\*Impacto en la Reputación\*\*: Las violaciones de seguridad pueden dañar la reputación de los comercios, llevando a la pérdida de clientes y disminución de ingresos.

## 4.3. Vulnerabilidad al Fraude

* \*\*Incremento en el Fraude\*\*: La falta de cumplimiento puede resultar en un aumento de las transacciones fraudulentas, lo que no solo afecta a los comercios, sino también a los consumidores y al ecosistema de pagos en general.

## 4.4. Desconexión del Ecosistema de Pagos

* \*\*Inhabilitación de Servicios\*\*: Los comercios que no cumplan con los requisitos pueden ser desconectados de la red de VISA, lo que les impediría procesar pagos a través de esta plataforma.

## Conclusión

Las nuevas reglas de VISA para la seguridad en comercio electrónico representan un cambio significativo en la forma en que los comercios y adquirentes deben operar. Es crucial que todas las partes involucradas se preparen adecuadamente para cumplir con estos requisitos, no solo para evitar sanciones, sino también para proteger la integridad del ecosistema de pagos y la confianza del consumidor. La implementación efectiva de estas medidas contribuirá a un entorno de comercio electrónico más seguro y eficiente.

# 4. Conclusiones

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

1. \*\*Adaptación Inminente y Proactiva\*\*: La implementación de las nuevas reglas de seguridad de VISA a partir de 2025 exige que los comercios, adquirentes y proveedores de servicios de pago realicen adaptaciones significativas en sus sistemas. La falta de preparación puede resultar en consecuencias severas, incluyendo multas y desconexión de la red de VISA. Por lo tanto, es imperativo que las entidades comiencen a evaluar y actualizar sus sistemas de manera proactiva.

2. \*\*Importancia de la Capacitación\*\*: La formación del personal es un aspecto crítico para garantizar el cumplimiento normativo. Los empleados deben estar bien informados sobre las nuevas extensiones de mensaje y los requisitos de participación en el programa CE 3.0. La capacitación adecuada no solo facilitará la implementación, sino que también ayudará a mitigar riesgos asociados al incumplimiento.

3. \*\*Riesgos Financieros y Reputacionales\*\*: El incumplimiento de las nuevas regulaciones puede acarrear riesgos financieros significativos, incluyendo multas y sanciones. Además, las violaciones de seguridad pueden dañar la reputación de los comercios, lo que podría traducirse en una pérdida de confianza por parte de los consumidores y, en consecuencia, en una disminución de ingresos. Es esencial que las entidades comprendan que la seguridad no solo es una obligación regulatoria, sino también un componente clave de su estrategia comercial.

4. \*\*Monitoreo y Auditoría Continua\*\*: Establecer mecanismos de monitoreo y auditoría interna será fundamental para asegurar que los sistemas y procesos se alineen con las nuevas especificaciones de VISA. Las pruebas de conformidad y la documentación precisa de las transacciones ayudarán a las entidades a mantenerse en cumplimiento y a facilitar auditorías futuras.

5. \*\*Colaboración en el Ecosistema de Pagos\*\*: La implementación de las nuevas reglas no solo recae en los comercios, sino que también implica una colaboración estrecha entre adquirentes, procesadores de pagos y proveedores de servicios. La facilitación de la implementación por parte de los proveedores de 3D Secure es crucial para el éxito general del cumplimiento normativo.

6. \*\*Enfoque en la Seguridad del Consumidor\*\*: La adopción de estas nuevas reglas tiene como objetivo final la creación de un entorno de comercio electrónico más seguro. Al cumplir con estas normativas, las entidades no solo protegen sus propios intereses, sino que también contribuyen a la seguridad y confianza del consumidor en el ecosistema de pagos.

7. \*\*Planificación Estratégica a Largo Plazo\*\*: Las entidades deben considerar la implementación de estas normas como parte de una estrategia de seguridad a largo plazo. Esto implica no solo cumplir con los requisitos actuales, sino también estar preparadas para futuras actualizaciones normativas y cambios en el panorama de seguridad en el comercio electrónico.

En resumen, las nuevas reglas de VISA representan un desafío significativo, pero también una oportunidad para mejorar la seguridad y la confianza en el comercio electrónico. La preparación adecuada y el cumplimiento proactivo son esenciales para navegar este cambio normativo de manera efectiva.

# 5. Recomendaciones

A continuación, se presentan recomendaciones prácticas y accionables para el cumplimiento de las nuevas reglas de seguridad de VISA para comercios electrónicos:

## Recomendaciones Prácticas para el Cumplimiento Normativo

## 1. \*\*Evaluación de Sistemas y Procesos\*\*

* Realizar una auditoría exhaustiva de los sistemas actuales para identificar brechas en relación con las nuevas reglas de seguridad de VISA.
* Desarrollar un plan de acción que incluya un cronograma para la actualización de sistemas y procesos necesarios para cumplir con las nuevas normativas.

## 2. \*\*Desarrollo de un Programa de Capacitación\*\*

* Implementar un programa de capacitación integral para todos los empleados, enfocado en las nuevas extensiones de mensaje y los requisitos del programa CE 3.0.
* Incluir simulaciones y escenarios prácticos que permitan a los empleados familiarizarse con los cambios y su aplicación en situaciones reales.

## 3. \*\*Gestión de Riesgos\*\*

* Establecer un marco de gestión de riesgos que evalúe tanto los riesgos financieros como reputacionales asociados con el incumplimiento normativo.
* Desarrollar un plan de respuesta a incidentes que contemple acciones a seguir en caso de violaciones de seguridad o incumplimientos.

## 4. \*\*Monitoreo y Auditoría Continua\*\*

* Implementar herramientas de monitoreo en tiempo real que permitan detectar y responder a posibles incumplimientos o vulnerabilidades en los sistemas.
* Programar auditorías internas periódicas para revisar la conformidad con las nuevas reglas y ajustar procesos según sea necesario.

## 5. \*\*Colaboración con Proveedores y Socios\*\*

* Establecer canales de comunicación claros con adquirentes, procesadores de pagos y proveedores de servicios para asegurar una implementación coordinada de las nuevas reglas.
* Participar en foros y grupos de trabajo de la industria para compartir mejores prácticas y mantenerse actualizado sobre las tendencias y cambios en la normativa.

## 6. \*\*Inversión en Tecnología de Seguridad\*\*

* Evaluar e invertir en tecnologías de seguridad avanzadas, como autenticación multifactor, cifrado de datos y sistemas de detección de fraudes, que fortalezcan la protección de las transacciones.
* Asegurarse de que las soluciones de 3D Secure estén actualizadas y alineadas con los requisitos de VISA.

## 7. \*\*Comunicación Transparente con los Consumidores\*\*

* Desarrollar una estrategia de comunicación que informe a los consumidores sobre las medidas de seguridad implementadas y cómo estas protegen sus datos y transacciones.
* Utilizar canales de comunicación como correos electrónicos, redes sociales y el sitio web para educar a los consumidores sobre la importancia de la seguridad en el comercio electrónico.

## 8. \*\*Planificación Estratégica a Largo Plazo\*\*

* Integrar el cumplimiento normativo en la planificación estratégica de la empresa, asegurando que se asignen recursos adecuados para la seguridad a largo plazo.
* Establecer un equipo de cumplimiento normativo que se encargue de monitorear cambios regulatorios y adaptar las políticas y procedimientos de la empresa en consecuencia.

## 9. \*\*Documentación y Registro\*\*

* Mantener una documentación detallada de todos los procesos, auditorías y capacitaciones realizadas para facilitar la verificación de cumplimiento en auditorías externas.
* Implementar un sistema de gestión de documentos que permita un fácil acceso y actualización de la información relacionada con el cumplimiento normativo.

## 10. \*\*Revisión y Actualización Continua\*\*

* Programar revisiones periódicas de las políticas y procedimientos de seguridad para asegurarse de que se mantengan alineados con las actualizaciones normativas y las mejores prácticas de la industria.
* Fomentar una cultura de mejora continua en la organización, donde todos los empleados se sientan responsables de la seguridad y el cumplimiento normativo.

## Conclusión

La implementación de estas recomendaciones no solo ayudará a los comercios a cumplir con las nuevas reglas de seguridad de VISA, sino que también fortalecerá su posición en el mercado al mejorar la confianza del consumidor y reducir riesgos asociados. La proactividad y la colaboración son clave para navegar con éxito este cambio normativo.

# 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 relevantes:

## 1. \*\*Especificaciones de Visa Secure\*\*

* Documentación oficial de VISA sobre las especificaciones de Visa Secure, incluyendo las nuevas extensiones de mensaje globales.

## 2. \*\*Compelling Evidence 3.0 (CE 3.0)\*\*

* Documentación que detalla el marco y los requisitos de la Evidencia Convincente 3.0, que es parte de las nuevas extensiones introducidas.

## 3. \*\*Intelligent Data Exchange (IDX)\*\*

* Información sobre el Intercambio de Datos Inteligentes, que forma parte de las nuevas especificaciones y su implementación.

## 4. \*\*Normativas de Autenticación de Visa\*\*

* Documentos que describen los programas de autenticación de Visa y los requisitos para la conformidad de las transacciones.

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

* Comunicados oficiales emitidos por VISA que anuncian la publicación y habilitación de las nuevas especificaciones, incluyendo las fechas clave mencionadas en el informe.

## 6. \*\*Guías de Implementación de VISA\*\*

* Guías y manuales que proporcionan detalles sobre cómo los adquirentes, comercios y 3DSS deben implementar las nuevas reglas y extensiones.

## 7. \*\*Regulaciones de Seguridad de Datos\*\*

* Normativas relacionadas con la seguridad de datos en el comercio electrónico que puedan influir en las prácticas de VISA, como el PCI DSS (Payment Card Industry Data Security Standard).

Incluir estas referencias ayudará a proporcionar un contexto más amplio y a respaldar la información presentada en el informe.