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

Un análisis detallado de las regulaciones y mejores prácticas para la protección de transacciones en línea

26/04/2025

# 1. Executive Summary

* Ejecutivo:\*\*

El informe detalla las actualizaciones normativas de Visa, efectivas a partir de octubre de 2024, que impactan a adquirentes, procesadores y emisores. Se introducen nuevas especificaciones bajo Visa Secure, que entrarán en vigor en abril de 2025, enfocadas en mejorar la seguridad de las transacciones electrónicas mediante la implementación de la Visa Additional Data Extension y la Visa Program Data Extension. Además, se establecen requisitos de control de sanciones que obligan a los miembros a revisar sus programas de cumplimiento. Por último, se actualiza el documento 'What To Do If Compromised' con recargos escalonados para comercios de Nivel 3, con el objetivo de fortalecer la seguridad del sistema de pagos ante compromisos de datos. Es esencial que los involucrados revisen los documentos disponibles en Visa Online para entender completamente los cambios y su impacto.

# 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 el ecosistema de pagos. Este documento está diseñado para ser una guía informativa para adquirentes, procesadores y emisores que operan en el ámbito del comercio electrónico y que deben cumplir con las normativas de VISA.

## Límites del Informe

1. \*\*Temporalidad\*\*: El informe se basa en la documentación y normativas disponibles hasta octubre de 2024, incluyendo las actualizaciones que entrarán en vigor en abril de 2025. No se abordarán cambios posteriores a esta fecha.

2. \*\*Enfoque en VISA\*\*: El análisis se centra exclusivamente en las reglas y normas de seguridad de VISA. No se incluirán comparaciones con otras redes de pago o regulaciones de seguridad de otras entidades.

3. \*\*Aspectos Técnicos\*\*: Aunque se mencionan especificaciones técnicas, el informe no profundiza en la implementación técnica de las nuevas extensiones de mensaje globales ni en los detalles operativos específicos para cada tipo de comercio.

4. \*\*Recomendaciones\*\*: Este informe no proporciona recomendaciones específicas para la implementación de las nuevas reglas, sino que se limita a describir los cambios y su impacto potencial. Las decisiones sobre la adopción de estas normas quedan a criterio de cada entidad involucrada.

5. \*\*Ámbito Geográfico\*\*: El informe se aplica a los comercios electrónicos que operan bajo la jurisdicción de VISA y no aborda las variaciones regionales o locales en la aplicación de estas normas.

Este alcance establece el marco dentro del cual se desarrollará el análisis, asegurando que los lectores comprendan el contexto y los límites de la información presentada.

# 3. Análisis Regulatorio

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

Este análisis se centra en las nuevas reglas de seguridad de VISA para comercios electrónicos, con un enfoque en los requisitos normativos, las obligaciones de las entidades reguladas, los procesos de cumplimiento necesarios y los riesgos asociados al incumplimiento.

## 1. Principales Requisitos Normativos Identificados

## 1.1 Actualización de Reglas y Normas de Visa

* \*\*Documentación\*\*: Las ediciones de octubre de 2024 de las Reglas Centrales de Visa y Normas de Información de Comercios son fundamentales para entender los cambios en la regulación.
* \*\*Impacto\*\*: Estas actualizaciones afectan a adquirentes, procesadores y emisores, lo que implica que todos los actores en la cadena de pagos deben estar al tanto de las modificaciones.

## 1.2 Visa Secure: Nuevas Extensiones de Mensaje Globales

* \*\*Visa Additional Data Extension\*\*: Introducción de especificaciones que soportan programas de autenticación como CE3.0 e IDX, con el objetivo de mejorar la seguridad de las transacciones.
* \*\*Visa Program Data Extension\*\*: Proporciona información sobre el cumplimiento de las transacciones con los programas de autenticación de Visa.

## 1.3 Requisitos de Control de Sanciones

* \*\*Obligación de Cumplimiento\*\*: Los miembros deben revisar y controlar periódicamente sus programas de control de sanciones para asegurar que no se provea a tarjetahabientes o comercios sujetos a sanciones.

## 1.4 Cambios en el Documento 'What To Do If Compromised'

* \*\*Recargos por Incumplimiento\*\*: Introducción de recargos escalonados para comercios de Nivel 3, alineando mejor los riesgos asociados a compromisos de datos.

## 1.5 Eliminación del Requisito de CAID Único

* \*\*Simplificación\*\*: Se elimina la necesidad de asignar un CAID único a ciertos comercios, facilitando el proceso de identificación de comerciantes.

## 2. Obligaciones para las Entidades Reguladas

## 2.1 Adquirentes, Procesadores y Emisores

* \*\*Revisión de Documentación\*\*: Deben revisar las ediciones de octubre de 2024 y aplicar los cambios necesarios en sus sistemas.
* \*\*Implementación de Nuevas Especificaciones\*\*: Prepararse para la habilitación de las nuevas extensiones de mensajes a partir de abril de 2025.

## 2.2 Control de Sanciones

* \*\*Monitoreo Continuo\*\*: Establecer un proceso de revisión periódica de los programas de control de sanciones para garantizar el cumplimiento.

## 2.3 Respuesta a Compromisos de Datos

* \*\*Adopción de Nuevas Políticas\*\*: Implementar las políticas actualizadas en el documento 'What To Do If Compromised', incluyendo la gestión de recargos por incumplimiento.

## 2.4 Identificación de Comerciantes

* \*\*Adaptación a Nuevos Marcos\*\*: Ajustar los procesos internos para alinearse con el nuevo marco Global Acceptor Identification Framework.

## 3. Procesos de Cumplimiento Necesarios

## 3.1 Evaluación de Impacto

* \*\*Análisis de Cambios\*\*: Realizar un análisis de impacto para identificar cómo las nuevas reglas afectan los sistemas y procesos existentes.

## 3.2 Capacitación y Concienciación

* \*\*Formación del Personal\*\*: Implementar programas de capacitación para asegurar que el personal esté al tanto de las nuevas regulaciones y procedimientos.

## 3.3 Implementación de Tecnología

* \*\*Actualización de Sistemas\*\*: Invertir en tecnología que soporte las nuevas especificaciones de Visa Secure y los requisitos de control de sanciones.

## 3.4 Auditorías Internas

* \*\*Revisiones Regulares\*\*: Establecer un calendario de auditorías internas para evaluar el cumplimiento con las nuevas normas y procedimientos.

## 4. Riesgos y Consecuencias del Incumplimiento

## 4.1 Riesgos Financieros

* \*\*Multas y Recargos\*\*: Las entidades que no cumplan con las nuevas regulaciones pueden enfrentar multas significativas y recargos escalonados, especialmente para comercios de Nivel 3.

## 4.2 Pérdida de Confianza

* \*\*Impacto en la Reputación\*\*: El incumplimiento puede resultar en una pérdida de confianza por parte de los consumidores y socios comerciales, afectando la reputación de la entidad.

## 4.3 Vulnerabilidad a Fraude

* \*\*Incremento de Riesgos de Seguridad\*\*: La falta de cumplimiento con las nuevas medidas de seguridad puede aumentar la vulnerabilidad a fraudes y compromisos de datos.

## 4.4 Consecuencias Legales

* \*\*Acciones Legales\*\*: Las entidades pueden enfrentar acciones legales por parte de consumidores o reguladores si no cumplen con las normativas de seguridad.

## Conclusiones

Las actualizaciones en las reglas de seguridad de VISA para comercios electrónicos representan un cambio significativo en el panorama de la regulación de pagos. Es crucial que todos los actores involucrados en el ecosistema de pagos comprendan y se adapten a estas nuevas normativas para mitigar riesgos y asegurar la integridad de las transacciones. Se recomienda consultar la documentación oficial en Visa Online para obtener información detallada y específica sobre cada uno de los cambios.

# 4. Conclusiones

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

1. \*\*Adaptación Obligatoria a Cambios Regulatorios\*\*: Las actualizaciones en las Reglas Centrales de Visa y Normas de Información de Comercios requieren que todos los actores en la cadena de pagos (adquirentes, procesadores y emisores) realicen una revisión exhaustiva de sus sistemas y procesos. La falta de adaptación puede resultar en sanciones financieras y comprometer la seguridad de las transacciones.

2. \*\*Mejora en la Seguridad de las Transacciones\*\*: La introducción de nuevas extensiones de mensaje, como la Visa Additional Data Extension y la Visa Program Data Extension, subraya el compromiso de VISA con la mejora de la seguridad en las transacciones electrónicas. Las entidades deben implementar estas especificaciones para fortalecer sus sistemas de autenticación y reducir el riesgo de fraudes.

3. \*\*Importancia del Control de Sanciones\*\*: La obligación de mantener programas de control de sanciones actualizados es crítica. Las entidades deben establecer procesos de monitoreo continuo para evitar la provisión de servicios a tarjetahabientes o comercios sujetos a sanciones, lo que podría acarrear graves consecuencias legales y financieras.

4. \*\*Gestión de Incidentes de Seguridad\*\*: La actualización del documento 'What To Do If Compromised' y la introducción de recargos escalonados para comercios de Nivel 3 enfatizan la necesidad de una respuesta efectiva ante compromisos de datos. Las entidades deben adoptar políticas claras y procedimientos de gestión de incidentes para mitigar el impacto de posibles brechas de seguridad.

5. \*\*Simplificación y Eficiencia en la Identificación de Comerciantes\*\*: La eliminación del requisito de CAID único para ciertos comercios representa un paso hacia la simplificación de procesos, lo que puede facilitar la identificación de comerciantes y mejorar la eficiencia operativa. Sin embargo, las entidades deben asegurarse de que sus sistemas se alineen con el nuevo marco Global Acceptor Identification Framework.

6. \*\*Inversión en Capacitación y Tecnología\*\*: La implementación de las nuevas regulaciones exige una inversión significativa en capacitación del personal y actualización de tecnología. Las entidades deben establecer programas de formación para garantizar que todos los empleados comprendan las nuevas normativas y estén preparados para cumplir con ellas.

7. \*\*Riesgos Asociados al Incumplimiento\*\*: Las consecuencias del incumplimiento son severas, incluyendo multas, pérdida de confianza del consumidor, vulnerabilidad a fraudes y posibles acciones legales. Las entidades deben ser proactivas en su enfoque hacia el cumplimiento normativo para evitar estos riesgos y proteger su reputación en el mercado.

8. \*\*Consulta Continua de Documentación Oficial\*\*: Es fundamental que las entidades consulten regularmente la documentación oficial de VISA para mantenerse actualizadas sobre los cambios normativos y asegurarse de que sus prácticas estén alineadas con las expectativas regulatorias.

En resumen, las nuevas reglas de seguridad de VISA para comercios electrónicos no solo representan un desafío, sino también una oportunidad para que las entidades fortalezcan sus sistemas de seguridad y mejoren la confianza del consumidor en el ecosistema de pagos. La adaptación efectiva a estas normativas es esencial para garantizar la integridad y seguridad de las transacciones electrónicas.

# 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 clave del análisis normativo:

## Recomendaciones Prácticas

## 1. \*\*Realizar un Diagnóstico de Cumplimiento\*\*

* \*\*Acción\*\*: Llevar a cabo una auditoría interna para evaluar el estado actual de los sistemas y procesos en relación con las nuevas reglas de VISA.
* \*\*Objetivo\*\*: Identificar brechas y áreas de mejora que requieran atención inmediata.

## 2. \*\*Actualizar Sistemas y Procesos\*\*

* \*\*Acción\*\*: Implementar las nuevas extensiones de mensaje (Visa Additional Data Extension y Visa Program Data Extension) en los sistemas de procesamiento de pagos.
* \*\*Objetivo\*\*: Aumentar la seguridad de las transacciones y reducir el riesgo de fraude.

## 3. \*\*Establecer un Programa de Control de Sanciones\*\*

* \*\*Acción\*\*: Desarrollar e implementar un programa de monitoreo continuo que incluya la verificación regular de listas de sanciones y la capacitación del personal sobre su importancia.
* \*\*Objetivo\*\*: Asegurar que no se presten servicios a tarjetahabientes o comercios sujetos a sanciones.

## 4. \*\*Desarrollar un Plan de Respuesta a Incidentes\*\*

* \*\*Acción\*\*: Crear y documentar un plan de gestión de incidentes que incluya procedimientos claros para la identificación, respuesta y notificación de brechas de seguridad.
* \*\*Objetivo\*\*: Minimizar el impacto de compromisos de datos y cumplir con las expectativas de VISA.

## 5. \*\*Revisar y Adaptar el Proceso de Identificación de Comerciantes\*\*

* \*\*Acción\*\*: Ajustar los sistemas internos para alinearse con el nuevo Global Acceptor Identification Framework, eliminando el requisito de CAID único donde sea aplicable.
* \*\*Objetivo\*\*: Mejorar la eficiencia operativa y la identificación de comerciantes.

## 6. \*\*Implementar Programas de Capacitación\*\*

* \*\*Acción\*\*: Desarrollar un programa de formación continua para todos los empleados sobre las nuevas regulaciones y su impacto en las operaciones diarias.
* \*\*Objetivo\*\*: Asegurar que el personal esté bien informado y preparado para cumplir con las normativas.

## 7. \*\*Establecer un Proceso de Monitoreo de Cumplimiento\*\*

* \*\*Acción\*\*: Designar un equipo responsable de la supervisión del cumplimiento normativo, que realice revisiones periódicas y mantenga registros de auditoría.
* \*\*Objetivo\*\*: Facilitar la identificación temprana de problemas de cumplimiento y garantizar la rendición de cuentas.

## 8. \*\*Mantenerse Actualizado con la Documentación Oficial\*\*

* \*\*Acción\*\*: Designar a un responsable de la consulta regular de la documentación oficial de VISA y de la implementación de cambios necesarios en los procesos internos.
* \*\*Objetivo\*\*: Asegurar que la entidad esté siempre alineada con las expectativas regulatorias y pueda adaptarse rápidamente a futuros cambios.

## 9. \*\*Evaluar Riesgos y Consecuencias del Incumplimiento\*\*

* \*\*Acción\*\*: Realizar un análisis de riesgos que contemple las posibles consecuencias del incumplimiento, incluyendo multas y pérdida de confianza del consumidor.
* \*\*Objetivo\*\*: Desarrollar estrategias proactivas para mitigar estos riesgos y proteger la reputación de la entidad.

## 10. \*\*Fomentar una Cultura de Cumplimiento\*\*

* \*\*Acción\*\*: Promover una cultura organizacional que valore el cumplimiento normativo y la seguridad de la información, incentivando la comunicación abierta sobre estos temas.
* \*\*Objetivo\*\*: Aumentar la conciencia y la responsabilidad en todos los niveles de la organización.

## Conclusión

La implementación de estas recomendaciones no solo ayudará a las entidades 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 la seguridad de las transacciones electrónicas. La proactividad en el cumplimiento normativo es esencial para el éxito a largo plazo en el ecosistema de pagos.

# 6. Referencias

Para la sección de referencias del informe normativo sobre las nuevas reglas de seguridad de VISA para comercios electrónicos, se pueden incluir las siguientes fuentes y documentos oficiales:

1. \*\*Reglas Centrales de Visa\*\* - Documentación oficial que detalla las normas y regulaciones que rigen las operaciones de VISA.

2. \*\*Normas de Información de Comercios\*\* - Documentación que proporciona directrices sobre la información que deben seguir los comercios al procesar transacciones.

3. \*\*Resumen de Cambios de Octubre de 2024\*\* - Documento que detalla las modificaciones específicas introducidas en la actualización de octubre de 2024.

4. \*\*Visa Secure\*\* - Documentación que describe el programa Visa Secure y sus especificaciones, incluyendo las nuevas extensiones de mensaje globales.

5. \*\*Visa Additional Data Extension\*\* - Especificación técnica que soporta programas de autenticación como la Evidencia Convincente (CE3.0) y el Intercambio de Datos Inteligentes (IDX).

6. \*\*Visa Online\*\* - Plataforma donde se pueden acceder a las ediciones más recientes de los documentos y normativas de VISA.

Estas referencias son esenciales para proporcionar un contexto adecuado y respaldar la información presentada en el informe.