INFORMACIÓN DE AFC

# Intercambio de información intersectorial sobre fraude

## Vías para la acción

Marzo de 2026

ACAMS

**Este documento se presentó al Grupo de Trabajo Internacional de Prevención del Fraude y Tecnología de ACAMS en febrero de 2026.**

# Resumen ejecutivo

El fraude se ha convertido en la principal amenaza contra los delitos financieros a nivel mundial, con pérdidas que continúan aumentando a pesar de una inversión organizacional sustancial. El desafío fundamental es claro: los esquemas de fraude operan en un vasto ecosistema que abarca las telecomunicaciones, las plataformas tecnológicas, las redes sociales, la banca y los mercados de criptomonedas. Sin embargo, la inteligencia sobre estos esquemas sigue aislada dentro de sectores y organizaciones individuales. Ninguna entidad individual ve el panorama completo, lo que hace que la interrupción en tiempo real sea casi imposible.

El **Grupo de Trabajo Internacional de Prevención del Fraude y Tecnología de ACAMS** decidió examinar el intercambio de información del sector privado para identificar el potencial de impacto operativo a corto plazo. La interrupción eficaz del fraude requiere inteligencia factible para llegar a las partes posicionadas y dispuestas a intervenir, lo que hace que una sólida infraestructura de intercambio de información sea un requisito previo para la prevención y respuesta coordinadas.

## Consideraciones principales y puntos de discusión para el Grupo de Trabajo

- **Iniciativas críticas:** En función de las oportunidades de acción identificadas, ¿existen iniciativas específicas en las que los miembros del grupo de trabajo sugieren que se priorice la acción, como una revisión en profundidad de cuestiones legales y de políticas sobre los permisos y las protecciones actuales en torno a los sectores, la privacidad y la responsabilidad? ¿Quién está mejor situado para avanzar en estos aspectos?

- **Apoyo a la colaboración:** ¿Qué organizaciones son las más adecuadas para asociarse a fin de iniciar el desarrollo de un marco de normas internacionales para el intercambio de información?

- **De cara al futuro:** ¿Cuáles son los elementos y las partes interesadas más críticos que se deben incluir, ya que ACAMS apoya al grupo de trabajo para (1) organizar el ejercicio de simulación para centrarse en la disponibilidad de información, el intercambio y las acciones en cada etapa del ciclo de vida del fraude, y (2) desarrollar el kit de herramientas de datos de fraude, que incluye plantillas de casos de uso de datos de alto valor específicos del sector y escenarios de fraude prioritarios (p. ej., prevención, interdicción, recuperación)?

## *Marcos existentes y barreras críticas*

Las participaciones de las partes interesadas en Estados Unidos, Europa y la región Asia-Pacífico revelan un patrón constante: el intercambio eficaz de información se puede lograr cuando está estructurado adecuadamente, pero las barreras sistémicas impiden que se escale. Donde funciona el intercambio, como a través de consorcios del sector financiero (p. ej., **Servicios de Alerta Temprana (EWS) Centro de Intercambio y Análisis de Información de Servicios Financieros (FS-ISAC)**, coaliciones tecnológicas (p. ej., el **Intercambio de Señales Globales**, el programa **Linterna de Coalición Tecnológica** que aborda la seguridad infantil), iniciativas intersectoriales como la plataforma **FINEST** de Hong Kong y el **Centro de Prevención de Estafas de Singapur**, y las asociaciones bilaterales, el éxito se deriva de una gobernanza clara, casos de uso enfocados, valor recíproco y relaciones de confianza.

Sin embargo, la gran mayoría de las organizaciones no comparten de manera efectiva la inteligencia sobre fraude. En una serie de participaciones y mesas redondas, los miembros de ACAMS y del grupo de trabajo identificaron las barreras más críticas para escalar la velocidad, la sofisticación, la capacidad de acción y la adopción del intercambio de información para combatir el fraude: la predisposición por parte del asesor legal de decir "no", los riesgos de responsabilidad percibida, la falta de permiso regulatorio claro, las incompatibilidades técnicas, las preocupaciones sobre la calidad de los datos y el daño reputacional, y, sobre todo, los limitados incentivos percibidos para invertir recursos en el intercambio voluntario que las instituciones consideran que pueden costar recursos significativos crean una responsabilidad potencial o incluso benefician a los competidores.

- **Incertidumbre legal y regulatoria:** Los puertos seguros de responsabilidad existentes concedidos por el Gobierno (por ejemplo, la Sección 314(b) de la Ley USA PATRIOT, la Ley de Intercambio de Información de Ciberseguridad) destinados a permitir el intercambio de información a escala están desaprovechados, con varios elementos que recibieron críticas por ser lentos, engorrosos, específicos del sector, restrictivos en su caso de uso y aplicación, o carecen de incentivos necesarios para promover el uso generalizado, incluso cuando algunos creen que el Gobierno ha dado amplias autoridades y protección. Las leyes de privacidad (por ejemplo, RGPD, CCPA, GLBA, ECPA) crean restricciones percibidas o reales, con una interpretación que varía drásticamente entre jurisdicciones y sectores, lo que exacerba aún más los problemas de intercambio transfronterizo. Las organizaciones informan que los equipos legales y de cumplimiento son reacios al riesgo, frenando iniciativas de intercambio de información antes de que comiencen.
- **Velocidad y oportunidad:** La infraestructura de fraude cambia constantemente, y los delincuentes monitorean continuamente las listas de bloqueos y cambian de dominios, números de teléfono y otras infraestructuras. Estos patrones hacen que los plazos diferidos para el intercambio de información sean ineficaces, en particular para la prevención e interdicción a corto plazo de los recursos provenientes de fraudes y estafas, que requieren una acción oportuna.
- **Incompatibilidad técnica y ausencia de normas:** Las organizaciones utilizan diferentes formatos de datos, identificadores y sistemas que dificultan el intercambio a escala actual de la información útil para combatir el fraude. En el ciclo de vida del fraude, diferentes informaciones son útiles para diferentes instituciones. Los formatos de los mensajes y las normas de datos varían según el país, la red y el tipo de datos (por ejemplo, la huella financiera o digital), lo que dificulta el intercambio de información eficaz.
- **Calidad de los datos y capacidad de acción:** Las organizaciones reciben con frecuencia inteligencia sin contexto suficiente. Sin puntajes de confianza, detalles de investigación y una guía práctica, los destinatarios no pueden justificar las decisiones operativas basadas en la inteligencia compartida. De manera más fundamental, muchas organizaciones también informan que no entienden qué información sería más útil para las organizaciones asociadas en otros sectores. Cuando se intercambió información en el pasado, muchas organizaciones expresaron su preocupación de que pareciera no haberse actuado conforme a ella ni producir resultados significativos.
- **Riesgo reputacional y preocupaciones competitivas**: Las organizaciones temen al daño reputacional y a la responsabilidad de bloquear a los clientes legítimos o ser percibidas como facilitadoras de la "desbancarización" o de negar el acceso a las comunicaciones o plataformas de redes sociales.
- **Silos y brechas de cobertura:** Si bien existe un intercambio eficaz de información en ámbitos específicos, el intercambio intersectorial sigue siendo mínimo, incluso cuando los estafadores explotan la infraestructura técnica, financiera y de comunicaciones intersectorial y transfronteriza. Romper los silos dentro de las organizaciones, pero especialmente en toda la industria y a nivel internacional, es fundamental para lograr el intercambio de información oportuno y factible.
- **Falta de incentivos organizacionales:** En la mayoría de los lugares y de los sectores, hay muy pocos incentivos para que las organizaciones participen en el intercambio de información intersectorial, y muchas organizaciones informan que se sienten desincentivadas para el intercambio porque las desventajas de este desde el punto de vista de los gastos de recursos, la posible responsabilidad y el riesgo reputacional superan cualquier beneficio.

## Próximos pasos

Abordar las barreras descritas anteriormente requerirá tanto mejoras operativas a corto plazo como cambios estructurales a largo plazo. Varias acciones a corto plazo podrían comenzar a mejorar el intercambio de información intersectorial sobre fraude: (1) aprovechar más eficazmente a las autoridades existentes, que incluyen explorar las revisiones legales formales de los permisos y protecciones actuales en todos los sectores, marcos de privacidad y responsabilidad; (2) identificar los tipos de información que son útiles para diferentes sectores; (3) intercambiar tipos de información de baja fricción, como alertas de tipología e identificadores hash, a través de sistemas automatizados que coincidan con la velocidad a la que operan los estafadores; (4) centrarse en datos de alto valor con el contexto para convertir los datos en inteligencia práctica; e (5) implementar plantillas de casos de uso y proyectos piloto para escenarios prioritarios basados en esquemas de fraude y casos de uso específicos en torno a la prevención, la interdicción o la recuperación. Para abordar los desafíos estructurales a largo plazo, los miembros del grupo de trabajo pueden considerar un esfuerzo específico para asignar e involucrar a las partes interesadas del sector público y privado a fin de abordar las aclaraciones legales y las brechas del puerto seguro, recurriendo a modelos internacionales exitosos.

Para apoyar al grupo de trabajo, ACAMS está desarrollando un **Kit de herramientas de datos de fraude** para mapear los elementos de datos útiles y prioritarios y su utilidad, y organizará un **ejercicio de simulación** para mapear más completamente los datos útiles, utilizar plantillas de casos de uso, y acciones preventivas y disruptivas habilitadas a lo largo del ciclo de vida de fraudes y estafas. ACAMS también trabajará a través del grupo de trabajo y de expertos externos para iniciar el **desarrollo de un marco de normas para el intercambio de información sobre fraude** definiendo casos de uso prioritarios, requisitos de elementos de datos e involucrando a organizaciones de estándares técnicos y no gubernamentales más amplias, organizaciones operativas y expertos para hacer la transición del marco hacia especificaciones técnicas formales para su adopción.

# Intercambio de información intersectorial sobre fraude: Caminos para la acción

## Antecedentes

El fraude aumentó drásticamente en los últimos años y fue identificado como la principal amenaza contra los delitos financieros a nivel global según el **Informe de ACAMS sobre las amenazas contra AFC a nivel global de 2026**. En la inauguración del Grupo de Trabajo Internacional de Prevención del Fraude y Tecnología de ACAMS, los miembros identificaron el intercambio de inteligencia entre partes privadas como una prioridad fundamental para la prevención coordinada del fraude.

Uno de los desafíos fundamentales en la lucha contra el fraude moderno es que las diferentes partes de los esquemas de fraude ocurren en un vasto ecosistema de fraude que incluye las telecomunicaciones, las plataformas tecnológicas, las redes sociales, la banca, los mercados de criptomonedas, entre otros sectores. Esta fragmentación deja a las empresas individuales con un panorama incompleto de lo que está sucediendo y dificulta la identificación del fraude, así como su interrupción en tiempo real.

A pesar de la inversión sustancial por parte de las organizaciones individuales, las pérdidas por fraude continúan aumentando a medida que las redes delictivas se adaptan rápidamente y operan a través de los límites organizacionales y jurisdiccionales. Las instituciones financieras, los proveedores de pagos, las plataformas tecnológicas, las empresas de telecomunicaciones y otras entidades privadas poseen inteligencia valiosa sobre patrones de fraude, infraestructura de perpetradores y objetivos de víctimas, pero esta información sigue estando en gran medida aislada. La inteligencia se intercambia de manera inconsistente, a menudo con demasiada lentitud para permitir una interrupción oportuna, y con frecuencia solo después de que ya se ha producido el fraude.

Una lección coherente de las asociaciones existentes es que el progreso se acelera una vez que las organizaciones son explícitas sobre qué datos deben intercambiarse, con quién, a qué velocidad y con qué propósito operativo. Cuando esta claridad está ausente, el intercambio de inteligencia se percibe como legalmente riesgoso, operacionalmente oneroso, sensible a la competencia o demasiado amplio, lo que lleva a las organizaciones a tomar precauciones en lugar de colaborar.

# Estado actual: Qué funciona y qué colapsa

## *Mecanismos de intercambio existentes*

La evidencia de múltiples sectores demuestra que el intercambio eficaz de información del sector privado se puede lograr cuando está estructurado adecuadamente:

- **Consorcios del sector financiero** como **EWS**, la **Australian Financial Crimes Exchange** y el **FS-ISAC** demostraron cómo el intercambio de inteligencia sobre las amenazas puede reducir las pérdidas por fraude mientras se respetan los límites competitivos. Su eficacia se deriva de varias características de diseño comunes: un enfoque en los indicadores de amenazas específicos en lugar de los datos de clientes, estructuras de gobernanza claras e incentivos que crean valor mutuo para los participantes.

> ***Caso de uso destacado: Las asociaciones facilitadas por el Gobierno***
>
> *Las plataformas facilitadas por el Gobierno en la región Asia-Pacífico proporcionan modelos para el intercambio intersectorial a escala. La plataforma **FINEST** de Hong Kong, gestionada de forma centralizada por la policía y que ahora incluye a bancos minoristas y virtuales, permite el intercambio automatizado entre partes múltiples de información de mulas de dinero y de cuentas fraudulentas con un impacto medible, lo que supuestamente reduce las solicitudes de suspensión de pagos desde el lanzamiento del proyecto piloto. Estas plataformas logran los objetivos a través de una autorización regulatoria explícita, una infraestructura técnica centralizada y procesos operativos claros.*

- **Las asociaciones de plataformas tecnológicas** han desarrollado acuerdos bilaterales para intercambiar inteligencia de cuentas y contenido que interrumpe las redes coordinadas de abusos. Las plataformas intercambian señales sobre cuentas fraudulentas, patrones de contenido fraudulento y comportamientos no auténticos coordinados que permiten a los socios tomar medidas proactivas antes de que el fraude aumente aún más.

> ***Caso de uso destacado: Las coaliciones tecnológicas intersectoriales***
>
> *Las coaliciones tecnológicas intersectoriales que abordan la seguridad infantil, como la Linterna de la Coalición Tecnológica, demuestran cómo la misión compartida y los requisitos normativos (sobre la base de que el material de abuso sexual infantil [CSAM] es un comportamiento universalmente condenado y legalmente obligado a abordarse) impulsan una colaboración eficaz que reúne a las instituciones financieras y las plataformas de redes sociales. La **Global Anti-Scam Alliance** y la **Global Signal Exchange (GSE)** facilitan la coordinación internacional sobre la inteligencia de estafas al consumidor, incluido el intercambio de indicadores técnicos como hashes de contenido y URL a través de GSE. Estos modelos funcionan porque la gravedad y la condena universal del problema, particularmente cuando se complementa con obligaciones legales, incentivan la participación.*

- **Las asociaciones de prevención del lavado de dinero** como la **Joint Money Laundering Intelligence Taskforce (JMLIT)** del Reino Unido y la **National Cyber-Forensics and Training Alliance (NCFTA)** demuestran que el intercambio impulsado por casos de uso con un alcance limitado y apoyado en relaciones de confianza produce un impacto medible. Estas iniciativas funcionan porque priorizan la inteligencia factible por encima del intercambio integral de datos.

> *Caso de uso destacado: Intercambio de información financiera ilícita de criptomonedas*
>
> *Han surgido varias asociaciones en la industria, algunas en asociación con entidades gubernamentales, para comenzar a operacionalizar el intercambio de información e incluso la recuperación de activos relacionados con ganancias derivadas de hechos ilícitos o estafas denominadas en criptomonedas con el fin de facilitar la recuperación, como la asociación **Illicit Virtual Asset Notification (IVAN)** la **Security Alliance (SEAL 911)**, **Operation Shamrock and the Crypto Coalition**, y el **T3** Programa de Colaboradores Globales de las Unidades de Delitos Financieros.*

- **Los acuerdos bilaterales informales** entre organizaciones individuales a menudo se mueven más rápido cuando surgen amenazas de fraude específicas, basándose en relaciones personales y un claro beneficio mutuo en lugar de marcos formales.

## *Dónde colapsa el intercambio*

A pesar de estos éxitos, existen barreras significativas que impiden una adopción más amplia:

- **Preocupaciones competitivas y déficits de confianza:** Como explicó un participante en la mesa redonda, "la confianza es difícil de escalar". A las organizaciones les preocupa que intercambiar inteligencia de fraude pueda revelar métodos de detección exclusivos, patrones de comportamiento de clientes o vulnerabilidades comerciales a los competidores. Los déficits de confianza entre los sectores y dentro de ellos limitan la voluntad de participar, particularmente cuando las organizaciones tienen obligaciones regulatorias o incentivos comerciales diferentes.
- **Incertidumbres legales y regulatorias:** Las leyes y regulaciones de privacidad (por ejemplo, el Reglamento General de Protección de Datos de la UE [RGPD], la Ley de Privacidad del Consumidor de California [CCPA], la Ley Gramm-Leach-Bliley [GLBA], la Ley del Derecho a la Privacidad Financiera [RFPA] y la Ley de Privacidad de las Comunicaciones Electrónicas [ECPA]), así como las consideraciones antimonopolio crean restricciones percibidas o reales sobre lo que puede compartirse. Las partes interesadas de los compromisos informaron constantemente que los equipos de las áreas de legales y cumplimiento son reacios al riesgo, lo que impide las iniciativas de intercambio de información antes de que comiencen. Incluso donde existen puertos seguros, las organizaciones informan que son lentas y engorrosas, con incentivos limitados y desincentivos prácticos; si intercambian información incorrectamente, enfrentan consecuencias regulatorias y reputacionales, pero muchas sienten que intercambiar con éxito no proporciona ningún beneficio organizacional. Sin embargo, otras partes interesadas destacaron las amplias protecciones de responsabilidad que ya se otorgaban a la industria en ciertas jurisdicciones para una serie de casos de uso, como los ejemplos estadounidenses de **314(b)** para las instituciones financieras que intercambian información para combatir el lavado de dinero o la **Ley de Intercambio de Información de Ciberseguridad** para el intercambio de información sobre ciberamenazas en el sector privado. Como señaló un participante, "se detiene en el área legal " debido a la interpretación conservadora de las regulaciones, incluso cuando existen la capacidad técnica y el deseo operativo de intercambiar.

Las dudas se profundizan con los desacuerdos entre las partes interesadas en torno a la claridad y el alcance de los marcos de responsabilidad y la aplicación del puerto seguro, así como las preocupaciones de responsabilidad sobre el intercambio de información que podría ser inexacta o intercambiar muy poco o demasiado tarde. Las protecciones de responsabilidad para diferentes sectores y los casos de uso están desaprovechados debido a estas restricciones percibidas o reales, así como a los incentivos limitados. Los diferentes sectores se enfrentan a diferentes restricciones legales, lo que hace que el intercambio intersectorial sea particularmente complejo.

- **Incompatibilidades técnicas:** Las inconsistencias en el formato de datos, los costos de integración de las API y la falta de estándares comunes hacen que el intercambio sea difícil desde el punto de vista operativo, incluso cuando se superan las barreras legales y de confianza. Las organizaciones utilizan diferentes identificadores para las mismas entidades, mantienen los datos a diferentes niveles de detalle y operan sistemas incompatibles. El desafío de la compatibilidad se extiende a nivel mundial y entre sectores. Incluso dentro de sectores individuales como las tarjetas de crédito, los sistemas de mensajes duales entre los bancos de titulares de tarjetas y los bancos mercantiles utilizan diferentes formatos, y cada país tiene sus propias redes y normas que no se alinean ni siquiera con las normas de la red de tarjetas. Lo que un pequeño banco regional encuentra útil difiere drásticamente de lo que necesitan las grandes instituciones, ya que las necesidades de las plataformas de telecomunicaciones y de redes sociales difieren de las necesidades de las instituciones financieras.
- **Preocupaciones de la calidad, confianza y aplicación de los datos:** Las organizaciones cuestionan si el intercambio de inteligencia será lo suficientemente preciso, oportuno y específico para justificar el esfuerzo operativo necesario para integrarlo y utilizarlo. Las partes interesadas hicieron hincapié en que los indicadores no procesados y sin contexto suelen tener un valor limitado. Por ejemplo, recibir una dirección de correo electrónico camboyana sin entender por qué es sospechoso o qué medidas tomar proporciona poca orientación práctica. Las organizaciones resaltaron la importancia de incluir puntajes de confianza u otros indicadores claros de confiabilidad para que los destinatarios puedan evaluar la información y priorizar su respuesta. Sin este contexto, los bancos que reciben inteligencia de plataformas tecnológicas pueden no estar seguros de cómo usarla. Los falsos positivos erosionan la confianza en las fuentes compartidas, mientras que la falta de retroalimentación sobre los resultados reduce el incentivo para continuar compartiendo.
- **Retrasos en la oportunidad:** Muchos acuerdos de intercambio existentes operan en ciclos diarios o semanales que son demasiado lentos para la prevención del fraude. Para el momento en que se intercambia la inteligencia, los estafadores ya trasladaron fondos, cerraron cuentas o cambiaron de tácticas e infraestructura. Para que el intercambio de información sea eficaz para prevenir el fraude en lugar de simplemente documentar pérdidas, debe automatizarse y operar a la velocidad y la escala de la actividad delictiva.
- **Brechas de cobertura:** Incluso cuando el intercambio funciona dentro de los sectores, el intercambio de inteligencia intersectorial sigue siendo limitado. Los bancos comparten con los bancos, las plataformas con las plataformas, pero el ecosistema del fraude abarca todos los sectores simultáneamente.
- **Preocupaciones de riesgo reputacional:** Las organizaciones temen que el daño reputacional bloquee o desbancarice a los clientes en función de la inteligencia compartida que podría ser incompleta o incorrecta. El riesgo de que un cliente que se haya retirado indebidamente genere una atención negativa en las redes sociales es una preocupación tan importante como la responsabilidad regulatoria o civil. Esto es particularmente crucial cuando las organizaciones carecen de información completa sobre si una persona es una víctima o un perpetrador, lo que hace que duden en tomar medidas sin realizar sus propias investigaciones. Estas preocupaciones se amplían en las jurisdicciones con una mayor sensibilidad pública sobre la exclusión financiera.

- **Falta de incentivos organizacionales:** Incluso cuando existen capacidad técnica y pasión individual, las organizaciones se enfrentan a una desalineación de incentivos fundamental. Como informaron algunas partes interesadas, "si los reguladores me dicen que debo hacerlo, lo haré, pero si no lo hacen, no lo haré". El intercambio voluntario de información requiere inversión de recursos (p. ej., revisión legal, integración técnica, procesos operativos) con un rendimiento incierto, lo que potencialmente beneficia a los competidores y expone a la organización que intercambia información a riesgos legales y reputacionales. Los accionistas cuestionan por qué las instituciones gastan recursos en iniciativas voluntarias. Sin mandatos claros o ventajas competitivas, las organizaciones se inclinan por cumplimiento mínimo en lugar de un intercambio proactivo.

## Priorizar la información que se intercambia

No todos los tipos de información se intercambian con el mismo nivel de valor o complejidad. Las organizaciones deben priorizar la extracción y el intercambio de información en función del impacto operativo y la viabilidad de la implementación.

### *Tipos de información de mayor valor*

En función de la participación de las partes interesadas, los tipos de información que se enumeran a continuación se identificaron como de prioridad alta para el intercambio intersectorial debido a su impacto operativo, su aplicabilidad intersectorial y su potencial para permitir la interrupción oportuna del fraude:

- **Identificadores de cuentas y destinos:** números de cuentas bancarias, nombres de originadores y beneficiarios, direcciones de billeteras de criptomonedas e identificadores de aplicaciones de pago para cuentas que reciben ganancias por fraude. Estos identificadores ayudan a permitir el bloqueo proactivo y los cierres coordinados.
- **Números de teléfono:** números utilizados para llamadas fraudulentas, mensajes de texto o verificación de cuentas que los proveedores de telecomunicaciones pueden bloquear y otros sectores pueden utilizar para señales de riesgo.
- **Redes de cuentas coordinadas:** identificadores de cuentas de plataformas y señales de comportamiento que muestran actividad fraudulenta coordinada en redes sociales, aplicaciones de citas u otros servicios.
- **Tipologías y tácticas de fraude:** descripciones de esquemas de fraude actuales, tácticas de ingeniería social y patrones de objetivos que permiten a las organizaciones actualizar las reglas de detección y advertir a las posibles víctimas.
- **Dominios e infraestructura:** URL, dominios, direcciones IP e información de hosting para sitios web fraudulentos e infraestructura de phishing que pueden eliminarse o bloquearse.
- **Identificadores de dispositivos y huellas digitales:** identificadores de dispositivos, rangos de direcciones IP sospechosas, huellas digitales del navegador, resolución de pantalla, patrones de presión de escritura y otras características del dispositivo que permiten el análisis de las redes.
- **Patrones de transacciones:** indicadores de comportamiento y secuencias de transacciones que distinguen el fraude de la actividad legítima sin revelar la identidad de los clientes.
- **Nombre y números de identificación nacionales:** nombres de clientes y números de identificación oficiales, como pasaportes, utilizados para cotejar entre bases de datos donde esté legalmente permitido.

*Nota sobre el nombre y los identificadores nacionales:* Si bien las organizaciones enfatizaron el valor de comenzar con estos identificadores básicos (por algunos identificados como "los puntos de datos más útiles" para generar coincidencias entre bases de datos organizacionales), reconocieron que las leyes de privacidad jurisdiccionales crean variaciones significativas para el intercambio. Estos puntos de datos tienen altas implicaciones de privacidad y requieren una justificación legal sólida. Otros resaltaron los desafíos con la compatibilidad entre regiones e idiomas para apoyar la resolución significativa y oportuna de la entidad.

## *Implicaciones legales por tipo de información*

Comprender el perfil de riesgo legal de los diferentes tipos de información ayuda a las organizaciones a priorizar qué compartir primero y qué requiere un análisis legal más cuidadoso. No toda la información relacionada con el fraude tiene las mismas implicaciones normativas o de privacidad. Una revisión inicial basada en la investigación y la participación de las partes interesadas permite discutir los niveles de riesgo para tipos de información específicos:

- **Riesgo de privacidad bajo:** Los indicadores de infraestructura de fraude, como los dominios y las direcciones IP, las descripciones de tipología de fraude y la información de patrones totales generalmente no implican datos personales y barreras legales mínimas.
- **Riesgo de privacidad moderado:** Los identificadores de cuentas hash o tokenizados, los números de teléfono asociados con un fraude confirmado y las direcciones de billeteras de criptomonedas implican datos personales, pero, a menudo, pueden compartirse según las disposiciones de prevención de fraude de las leyes de privacidad con las protecciones adecuadas.
- **Riesgo de privacidad alto:** Los datos de las cuentas de clientes no cifrados, el contenido de las comunicaciones, los historiales de transacciones y la vinculación de múltiples identificadores a personas requieren un análisis legal cuidadoso y una justificación más sólida según los principios de necesidad y proporcionalidad.

Las diferentes jurisdicciones y sectores tienen diferentes permisos de referencia para intercambiar la información a través de las fronteras y con diferentes autoridades. Las instituciones financieras que operan según la Ley Gramm-Leach-Bliley (GLBA) en los Estados Unidos tienen una autoridad más clara para el intercambio relacionado con el fraude que muchos otros sectores, mientras que los proveedores de telecomunicaciones se enfrentan a restricciones más estrictas según la Ley de Privacidad de las Comunicaciones Electrónicas (ECPA). En la Unión Europea, el artículo 6(1) (f) del RGPD proporciona una base de interés legítimo que se aplica en todos los sectores, pero la interpretación varía significativamente según el estado miembro y la autoridad de protección de datos. El marco de Singapur autoriza explícitamente el intercambio de información entre bancos y proveedores de telecomunicaciones a través del Centro de prevención de estafas, mientras que las excepciones de la Ley de Privacidad de Australia para la prevención del fraude siguen sujetas a una interpretación variada entre sectores. Estas diferencias jurisdiccionales y sectoriales significan que un número de teléfono compartido por un proveedor de telecomunicaciones del Reino Unido puede enfrentar diferentes consideraciones legales que el mismo número compartido por una institución financiera estadounidense, incluso cuando ambos actúen para prevenir el mismo esquema de fraude.

### *Mayor retorno de la inversión (ROI) para el intercambio*

El intercambio de información prioritario debe centrarse en información que sea:

- **Crítica para el momento de la interrupción:** El intercambio en tiempo real o por hora de la infraestructura activa de fraude permite bloquear antes de que se produzca un daño significativo a la víctima.
- **Intersectorial:** Los números de teléfono, las direcciones de billeteras y los dominios son útiles para varios sectores, lo que maximiza el valor del intercambio.
- **Claramente aplicable:** La inteligencia que permite acciones de protección específicas, como bloquear pagos, eliminar una cuenta o advertir a los clientes, justifica la inversión operativa.
- **Ya recopilada:** La información que las organizaciones mantienen para su propia prevención del fraude requiere un costo adicional mínimo para su intercambio.
- **Más clara jurídicamente:** Comenzar con tipos de información de menor riesgo genera confianza y capacidad operativa antes de abordar escenarios más complejos.
- **Contextualmente completa:** La inteligencia que se intercambia con contexto aplicable, como los puntajes de confianza, detalles de investigación y orientación clara sobre qué medidas pueden tomar los destinatarios (p. ej., bloquear un pago, congelar una cuenta, eliminar contenido, advertir a los clientes) justifica la inversión operativa de manera mucho más eficaz que los puntos de datos sin procesar.

Con prioridades establecidas en torno a los tipos de información más valiosos y legalmente viables, las organizaciones pueden tomar medidas inmediatas utilizando las autoridades existentes y enfoques de baja fricción.

## Oportunidades a corto plazo

Se discutieron varias oportunidades que podrían mejorar el intercambio de información sin requerir nueva legislación ni grandes inversiones técnicas.

### *Mejorar el uso de las autoridades legales existentes*

Muchas organizaciones desaprovechan los permisos legales existentes que proporcionan diversas protecciones y permisos para intercambiar cierta información sobre el fraude y relacionada con él:

- **La sección 314(b) de la Ley USA PATRIOT** establece un puerto seguro para que las instituciones financieras compartan información relacionada con el fraude, pero sigue estando desaprovechada debido a la falta de conocimiento o una interpretación demasiado prudente.
- **La Ley de Intercambio de Información de Ciberseguridad de 2015** establece protecciones de responsabilidad intersectorial para intercambiar información relacionada con ciberamenazas y medidas defensivas. A diferencia de la Sección 314(b), que se aplica principalmente a las instituciones financieras, CISA cubre a cualquier miembro del sector que intercambie información sobre amenazas cibernéticas. Dado que la mayoría de los fraudes modernos están habilitados para la cibernética, este puerto seguro existente puede proporcionar una autoridad más amplia para el intercambio de inteligencia sobre fraude entre sectores que la autoridad que las organizaciones reconocen actualmente.
- **La base de "intereses legítimos" del artículo 6(1)(f) del RGPD** permite el procesamiento de la prevención del fraude, pero las organizaciones a menudo adoptan enfoques innecesariamente conservadores sin buscar opiniones legales que confirmen la permisibilidad.

- **Las disposiciones específicas del sector** en las regulaciones contra el fraude en las telecomunicaciones, las reglas de los sistemas de pago (como las regulaciones operativas de las redes de tarjetas) y los términos de servicio de las plataformas a menudo permiten un intercambio más amplio de lo que las organizaciones creen, pero es posible que no se entiendan bien fuera de sus respectivos sectores.
- **Los mecanismos contractuales**, incluidos los acuerdos de confidencialidad (NDA), los acuerdos bilaterales de intercambio de datos y las estructuras de membresía de consorcios, pueden abordar muchas preocupaciones de confidencialidad y responsabilidad sin requerir de nueva legislación, aunque requieren de recursos legales para negociar e implementar de manera eficaz.

Las organizaciones podrían realizar revisiones legales multifuncionales con la participación de abogados de todas las jurisdicciones relevantes para establecer bases de referencia de intercambio que documenten lo que se puede compartir hoy en día según los marcos existentes. La facilitación regulatoria puede acelerar la utilización de las autoridades existentes. En Hong Kong, los reguladores bancarios proporcionaron cartas explícitas a los bancos participantes para confirmar que el intercambio de información para la prevención del fraude estaba permitido incluso antes de que se finalizaran las enmiendas a la ley de privacidad, lo que creó la comodidad legal necesaria para lanzar la plataforma FINEST. Esto demuestra que los reguladores pueden permitir la acción dentro de los marcos existentes a través de una comunicación clara y una autorización explícita, sin esperar a que se produzcan cambios legislativos.

## *Tipos de información de baja fricción para el intercambio inmediato*

Las organizaciones pueden comenzar de inmediato con tipos de información que enfrentan barreras legales u operativas mínimas, las que pueden incluir:

- **Alertas de tipología de fraude:** las descripciones de los esquemas de fraude, las tácticas y los patrones de objetivos actuales no implican datos personales y pueden compartirse libremente a través de los canales de comunicación existentes.
- **Identificadores hash:** los números de teléfono, los números de cuentas y las direcciones de billeteras hash que utilizan algoritmos comunes proporcionan una capacidad de coincidencia significativa con protección de la privacidad y una complejidad técnica mínima.
- **Indicadores de infraestructura:** los dominios, las URL, las direcciones IP y la información de hosting de sitios fraudulentos confirmados se pueden compartir para efectos de bloqueo y coordinación de su desactivación.
- **Patrones agregados:** la información estadística sobre tendencias de fraude, concentraciones geográficas y patrones temporales permite una detección mejorada sin revelar los registros individuales.

Las organizaciones hicieron hincapié en que para la información que no permite la identificación personal (información no PII), como alertas de tipología de fraude, indicadores de infraestructura y patrones agregados, el intercambio debe automatizarse para que coincida con la velocidad a la que operan los delincuentes. Los procesos manuales para revisar y aprobar el intercambio de dominios, direcciones IP e información de tipología introducen retrasos que hacen que la inteligencia se vuelva obsoleta. Los sistemas automatizados pueden intercambiar estos tipos de información de bajo riesgo a la velocidad y escala necesarias. Estos tipos de información de bajo riesgo pueden intercambiarse inmediatamente a través de canales informales o acuerdos bilaterales simples, lo que crea capacidad operativa y confianza para escenarios de intercambio más complejos.

### *Pilotos y plantillas*

Desarrollar y promover la adopción de plantillas y guías específicas como parte de programas piloto o implementaciones más amplias, podría proporcionar herramientas prácticas a corto plazo que sean útiles para quines combaten el fraude de primera línea, como pueden ser:

- **Plantillas de casos de uso:** documentación detallada para tres a cinco escenarios de intercambio prioritario (cuentas de mulas de banco a banco, de banco a direcciones de billeteras de criptomonedas, números de teléfono de estafas de telecomunicaciones a todos, cuentas coordinadas de plataforma a plataforma y estafadores de romance de aplicaciones de citas a bancos) que especifique qué elementos de datos se deben compartir, la base legal, los requisitos de la oportunidad y las acciones habilitadas.
- **Documentos de orientación legal:** análisis por jurisdicción de los permisos de intercambio existentes, acuerdos de intercambio de datos de plantillas y explicaciones de las disposiciones de puerto seguro.
- **Guías técnicas:** especificaciones simples para el intercambio de identificadores hash, estructuras API para el intercambio bilateral y esquemas de datos mínimos viables.
- **Plantillas de gobernanza:** modelos de contratos para acuerdos bilaterales, de consorcios e intermediarios con términos estándar de reciprocidad, restricción de uso y rendición de cuentas.
- **Programas piloto:** el lanzamiento de tres a cinco pilotos coordinados para probar escenarios de intercambio de prioridades con participantes voluntarios, donde se documenten los desafíos de implementación y las lecciones aprendidas para una reproducción más amplia.

## Desafíos estructurales a largo plazo

Si bien es posible lograr avances a corto plazo con las autoridades existentes, varias barreras requieren marcos más formales y medidas legislativas o regulatorias.

### *Puertos seguros y protecciones de responsabilidad*

**Brecha actual:** Los puertos seguros existentes son específicos del sector, principalmente para las instituciones financieras, y no cubren claramente el intercambio intersectorial. Las organizaciones temen que se les adjudique responsabilidad por intercambiar información inexacta, compartir muy poco o hacerlo demasiado tarde.

**Qué se necesita:** Las disposiciones de puertos seguros explícitas deben permitir el intercambio de información sobre fraude entre sectores, incluidos bancos, plataformas, empresas de telecomunicaciones, sectores minoristas y mercados de criptomonedas, según las condiciones específicas. Las protecciones de responsabilidad para el intercambio de buena fe deben ser lo suficientemente claras y sólidas como para reducir las dudas organizacionales.

**Ejemplos de enfoques existentes:**

- **Estados Unidos:** La Sección 314(b) de la Ley USA PATRIOT establece un puerto seguro para las instituciones financieras, pero no se extiende claramente al intercambio intersectorial con plataformas, ni a proveedores de telecomunicaciones o instituciones no financieras. La Ley de Intercambio de Información de Ciberseguridad de 2015 establece protecciones de responsabilidad para cualquier miembro de la industria por intercambiar información relacionada con ciberamenazas y medidas defensivas, que podrían extenderse a los indicadores de fraude cibernéticos.

- **Australia:** La Ley de Privacidad australiana contiene excepciones para la prevención del fraude, pero la interpretación varía y la aplicación intersectorial sigue siendo incierta.
- **Hong Kong:** La Oficina de Inteligencia e Investigación Financiera, a través de la policía de Hong Kong, opera la plataforma FINEST, que recibió autorización regulatoria explícita a través de cartas emitidas por la Autoridad Monetaria de Hong Kong a los bancos participantes para confirmar que el intercambio estaba permitido con fines de prevención del fraude. La plataforma ahora incluye a todos los bancos minoristas y bancos virtuales en un sistema de intercambio centralizado y automatizado de muchos a muchos a fin de conocer información sobre mulas de dinero y cuentas fraudulentas, lo que generó una reducción mensurable en los niveles de fraude desde su implementación.
- **Singapur:** El Marco de responsabilidad compartida para estafas de phishing crea una autoridad explícita para que los proveedores de servicios de telecomunicaciones y los bancos intercambien información a través del Centro de Prevención de Estafas.
- **Corea del Sur:** Un marco de prevención del fraude integral dirigido por las autoridades de aplicación de la ley y los organismos reguladores financieros reúne a bancos, instituciones financieras no bancarias, empresas de tecnología financiera y proveedores de telecomunicaciones con autoridad de congelamiento inmediato de cuentas cuando se identifica un caso de fraude. El marco demuestra cómo la acción legislativa que crea autoridad clara, mecanismos de aplicación sólidos y coordinación intersectorial puede impulsar la participación sistemática.

**Consideraciones principales:** Desarrollar puertos seguros intersectoriales que permitan intercambiar indicadores de fraude específicos, como identificadores de cuentas, números de teléfono, direcciones de billeteras e indicadores de infraestructura, entre los sectores designados según la gobernanza adecuada, con protección de responsabilidad para un intercambio de buena fe que cumpla con las normas definidas.

## *Aclaraciones de la Ley de Privacidad y Antimonopolio*

**Aclaraciones de privacidad posible:**

- Orientación clara de que la prevención del fraude constituye un interés legítimo u otra base legal según el RGPD y otros marcos similares.
- Orientación clara sobre cómo se aplican las disposiciones de prevención del fraude en los diferentes sectores, como los servicios financieros, las telecomunicaciones, las plataformas tecnológicas y los sectores minoristas.
- Permiso explícito para intercambiar inteligencia de fraude transfronterizo según las regulaciones de transferencia de datos.
- Orientación de proporcionalidad que especifica los elementos de datos que son razonables para su intercambio en diferentes escenarios de fraude.
- Disposiciones de velocidad y oportunidad que reconocen que el intercambio tardío puede hacer que la inteligencia no sea de utilidad.

**Aclaraciones de antimonopolios posibles:**

- Confirmación de que intercambiar información sobre amenazas de fraude no constituye un intercambio de información anticompetitivo.
- Orientación sobre estructuras de gobernanza adecuadas para los consorcios del sector.
- Límites claros entre el intercambio permitido de indicadores de fraude y el intercambio no permitido de información comercial.

**Ejemplos:**

- **Unión Europea:** Las autoridades de protección de datos podrían emitir directrices coordinadas sobre el intercambio de información sobre prevención del fraude similares a las directrices emitidas para el procesamiento de datos de COVID-19.

- **Estados Unidos:** La Comisión Federal de Comercio y el Departamento de Justicia podrían aclarar los límites antimonopolio para los consorcios de intercambio de información sobre fraude.

**Consideraciones principales:** Colaborar con las autoridades de protección de datos y los entes reguladores de la competencia para desarrollar directrices específicas que aclaren los permisos y límites existentes para el intercambio de inteligencia sobre fraude. Esto ayudará a reducir el riesgo legal percibido que impide la acción según los marcos existentes.

## *Autoridades de intercambio de datos transfronterizos*

**Brecha actual:** El intercambio de inteligencia sobre fraude transfronterizo se enfrenta a la incertidumbre según las restricciones de transferencia de datos (p. ej., requisitos de adecuación del RGPD, implicaciones de Schrems II, requisitos de localización de datos sectoriales). Las organizaciones a menudo no intercambian información a nivel internacional, incluso cuando es esencial desde el punto de vista operativo. A pesar de estos desafíos, existen marcos y obligaciones de tratados que respaldan el intercambio de información legal transfronterizo (por ejemplo, Grupo Egmont de las UIF, La Convención de las Naciones Unidas contra el Ciberdelito, Tratados de Asistencia Legal Mutua).

**Qué se necesita:** Los mecanismos deben permitir el intercambio internacional de inteligencia sobre fraude en tiempo real que funcione dentro de los marcos de protección de datos existentes. Esto podría incluir el reconocimiento mutuo de la prevención del fraude como una protección adecuada, cláusulas contractuales estándar específicamente para la inteligencia del fraude o marcos multilaterales similares a las Reglas de Privacidad Transfronteriza de APEC.

**Ejemplos:**

- **Región Asia-Pacífico:** La iniciativa FRONTIER+ demuestra el intercambio de inteligencia de estafas transfronterizo, pero carece de un marco legal integral.
- **Europa-EE. UU.:** El Marco de Privacidad de Datos proporciona un mecanismo para las transferencias transatlánticas de datos, pero la aplicación del intercambio de inteligencia sobre fraude sigue siendo poco clara.

**Consideraciones principales:** Desarrollar marcos modelo para el intercambio transfronterizo de inteligencia sobre fraude que satisfagan los requisitos de protección de datos mientras permitan la velocidad operativa, potencialmente a través de acuerdos multilaterales entre Gobiernos o acuerdos de reconocimiento mutuo entre entes reguladores. Proponer un lenguaje de políticas a organizaciones como el Grupo de Acción Financiera Internacional (GAFI) para integrar el intercambio transfronterizo oportuno de transacciones e información auxiliar como fundamental para combatir el delito financiero y el lavado de dinero, como en las actualizaciones de la Recomendación 16.

## *Responsabilidad, mandatos y requisitos regulatorios*

Varias jurisdicciones fueron más allá del intercambio voluntario para crear obligaciones regulatorias, que cambiaron fundamentalmente los incentivos de participación.

**Desafío:** Es posible que los enfoques voluntarios no logren una participación o inversión suficientes cuando las presiones competitivas desalientan la acción.

**Cómo funciona:** Los requisitos legales y regulatorios crean obligaciones de prevención del fraude y de intercambio de información para las empresas en todos los sectores, con sanciones significativas y responsabilidad por incumplimiento de las normas.

**Efecto previsto:** Las empresas aumentan la inversión en controles de fraude e iniciativas de intercambio de información intersectorial, lo que conduce a una mejor identificación y disrupción del fraude, menores pérdidas por fraude en general y una mayor recuperación de activos para las víctimas. Cuando las empresas se enfrentan a posibles sanciones significativas, invierten en sus propios controles y se aseguran de que otros participantes en línea ascendente y descendente compartan información para mitigar su riesgo.

**Ejemplos:**

- **Singapur:** El Marco de Responsabilidad Compartida para Estafas de Phishing crea responsabilidad para los bancos y proveedores de servicios de telecomunicaciones que no cumplen con las obligaciones especificadas de prevención de fraude e intercambio de información, lo que incentiva la participación proactiva en el Centro de prevención de estafas.
- **Reino Unido:** El reembolso obligatorio de las estafas por Fraude de pago autorizado (Authorized Push Payment, APP) crea un incentivo financiero para que los proveedores de servicios de pago inviertan en la prevención del fraude y participen en el intercambio de información para reducir su exposición a la responsabilidad.
- **Unión Europea:** Los sólidos requisitos de autenticación de clientes PSD2 y las obligaciones de monitoreo del fraude crean estándares de referencia, aunque el intercambio de información sigue siendo en gran medida voluntario.

**Compensaciones:** Los mandatos impulsan la inversión y la participación, pero corren el riesgo de ser prescriptivos y pueden no adaptarse rápidamente a las tácticas de fraude en evolución. Funcionan mejor cuando se combinan con las aportaciones del sector sobre la implementación y la flexibilidad para que las organizaciones elijan cómo cumplir con los requisitos basados en los resultados.

**Consideraciones principales:** En jurisdicciones donde los enfoques voluntarios resultan insuficientes, considere los requisitos regulatorios basados en los resultados (p. ej., reducir las pérdidas por fraude, mejorar los tiempos de respuesta, participar en el intercambio de información) en lugar de los mandatos prescriptivos, lo que permite a las organizaciones flexibilidad en la implementación mientras crean una rendición de cuentas clara para los resultados.

## Mecanismos de incentivos voluntarios

Más allá de los mandatos regulatorios, existen varios enfoques que pueden incentivar la participación sin necesidad de requisitos legales.

### *Normas y compromisos voluntarios del sector*

**Desafío:** Mejorar los controles de fraude y participar en el intercambio de información puede crear una desventaja competitiva cuando otros miembros del mismo sector no toman medidas similares.

**Cómo funciona:** Las empresas se comprometen voluntariamente a cumplir las normas o requisitos para promover el intercambio de información sobre fraude. Estas normas podrían aplicarse dentro de un sector o entre sectores, lo que se ve facilitado por las asociaciones del sector, el estímulo gubernamental o la acción colectiva de las principales organizaciones.

**Efecto previsto:** Si la participación es lo suficientemente alta, reduce la desventaja competitiva. Esto sube el listón en todos los sectores y presiona a las empresas que de otro modo no se predisponen a mejorar los controles de fraude para evitar que el Gobierno, las entidades reguladoras o el público las perciban como casos atípicos del sector que no se comprometen a combatir el fraude y proteger a los clientes. Esto puede servir como un primer paso hacia iniciativas de intercambio de información más amplias.

**Ejemplos:**

- **Reino Unido:** La Carta del Sector de Prevención del Fraude en las Telecomunicaciones reúne a los proveedores de telecomunicaciones para comprometerse a implementar medidas de prevención del fraude específicas y prácticas de intercambio de información.
- **Estados Unidos:** Asociaciones del sector, como la Asociación de Banqueros Estadounidenses, promueven el intercambio de información sobre fraude a través de iniciativas como EWS y FS-ISAC.
- **A nivel global:** Las reglas de fraude de las redes de tarjetas de pago crean estándares de facto para las instituciones financieras participantes, y las organizaciones globales permiten compartir indicadores técnicos (p. ej., GSE).

### *Iniciativas del sector privado*

**Desafío:** La colaboración intersectorial es difícil. Navegar por los desafíos legales, normativos y operativos requiere tiempo y recursos que las organizaciones individuales luchan por justificar.

**Cómo funciona:** El sector privado forma organizaciones, asociaciones o grupos para facilitar y ejecutar el intercambio de información sobre fraude entre sectores. El Gobierno puede reconocer, alentar o respaldar estas iniciativas y puede participar en ellas.

**Efecto previsto:** Hacer que una organización navegue colectivamente los desafíos en nombre de los miembros es más eficaz y eficiente. Permite una identificación del fraude más rápida y precisa, y una mayor velocidad en la adopción de acciones disruptivas en todos los sectores, como cerrar cuentas bancarias, bloquear números de teléfono, y eliminar cuentas y sitios en línea.

**Ejemplos:**

- **Reino Unido:** CIFAS es una organización de membresía sin ánimo de lucro que reúne a la banca, los seguros, las telecomunicaciones, el sector minorista y el Gobierno, y proporciona un marco para el intercambio en tiempo real de datos e inteligencia de riesgo de fraude.
- **Reino Unido:** STOP Scams UK es una organización miembro de empresas bancarias, tecnológicas y de telecomunicaciones, que facilita la colaboración intersectorial para luchar contra las estafas.
- **Estados Unidos:** La NCFTA (National Cyber-Forensics and Training Alliance) opera como una asociación entre el sector, las autoridades de aplicación de la ley y el mundo académico para compartir inteligencia sobre delitos cibernéticos y fraude.

## *Iniciativas dirigidas por el Gobierno*

**Desafío:** Las iniciativas del sector privado pueden carecer de suficiente autoridad, conocimientos especializados o coordinación con las autoridades de aplicación de la ley para permitir una rápida disrupción y recuperación de activos.

**Cómo funciona:** El Gobierno crea células de fusión y centros de inteligencia que reúnen a los sectores público y privado, a menudo con la misma ubicación física, para compartir información, conocimientos e inteligencia relacionada con el fraude.

**Efecto previsto:** Como intermediario de confianza, el liderazgo gubernamental puede reducir la incertidumbre legal y regulatoria. Estas iniciativas pueden permitir al Gobierno recibir y compartir información de manera más eficiente y alinear las actividades con las prioridades gubernamentales. Pueden aumentar la velocidad de la disrupción y la recuperación de activos, y facilitar que el Gobierno proporcione comentarios a empresas del sector privado.

**Ejemplos:**

- **Australia:** El Centro Nacional de Prevención de Estafas (NASC) reúne a agencias gubernamentales, autoridades de aplicación de la ley, bancos, proveedores de telecomunicaciones y plataformas tecnológicas para compartir inteligencia y coordinar respuestas en tiempo real.
- **Singapur:** El Centro de Prevención de Estafas (ASC) opera como una iniciativa pública-privada conjunta con representantes en la misma ubicación de bancos, proveedores de telecomunicaciones y autoridades de aplicación de la ley para permitir el intercambio inmediato de la información y la disrupción coordinada.
- **Reino Unido:** JMLIT (Joint Money Laundering Intelligence Taskforce) y el Grupo de Trabajo Conjunto contra el Fraude proporcionan modelos para la fusión de la inteligencia público-privada.

Cada enfoque tiene fortalezas y limitaciones. Las iniciativas dirigidas por el Gobierno a menudo ofrecen los beneficios de una mayor prioridad y autoridad para obtener efectos más duraderos, mientras enfrentan desafíos relacionados con la agilidad y la oportunidad necesarias ante las amenazas más adaptativas y a corto plazo. Los modelos más exitosos combinan elementos clave como la claridad legal de referencia a través de puertos seguros, el liderazgo voluntario del sector a través de normas e iniciativas del sector privado, la facilitación del Gobierno a través de centros de fusión y los requisitos obligatorios específicos cuando los enfoques voluntarios resultan insuficientes.

# Requisitos técnicos y de gobernanza

## *Infraestructura técnica*

Las organizaciones necesitan una infraestructura que equilibre la utilidad operativa, la seguridad, la protección de la privacidad y la viabilidad de la implementación. Por ejemplo:

- **Algunos requisitos principales para los esfuerzos de intercambio de información a corto plazo:**
    - Canales de transmisión seguros (p. ej., TLS, VPN)
    - Capacidades básicas de coincidencias para identificadores clave
    - Esquemas de datos claros que definan los formatos y significados de los campos
    - Controles de acceso que garanticen que solo el personal autorizado pueda consultar o recibir inteligencia
    - Registros de auditoría para apoyar la rendición de cuentas
    - Mecanismos de comentarios para informar sobre las acciones tomadas
- **Normas técnicas prioritarias que podrían apoyar la infraestructura de intercambio de información:**
    - Formatos de identificadores comunes para números de cuentas, números de teléfono, direcciones de billeteras de criptomonedas, dominios y direcciones IP
    - Una taxonomía común de tipología del fraude que se traduzca en todos los sectores
    - Indicadores de confianza y calidad para la inteligencia compartida
    - Formatos para reportar acciones y resultados
    - Especificaciones de la API para el intercambio bilateral
    - Orientación sobre técnicas de preservación de la privacidad (p. ej., uso de hash, tokenización y cuándo usar cada una)

**Oportunidades inmediatas:** Las organizaciones pueden comenzar inmediatamente con identificadores hash simples y explorando el uso de los algoritmos comunes. Esto proporciona una protección de privacidad significativa y permite la coincidencia entre organizaciones sin requerir una infraestructura sofisticada o una revisión legal.

## *Requisitos de gobernanza*

**Principios básicos de gobernanza:** Los acuerdos de intercambio de información funcionan de manera más eficaz cuando siguen un conjunto de principios que fomentan la confiabilidad y la seguridad en todo el entorno de intercambio:

- **Reciprocidad:** Las organizaciones que reciben inteligencia deben contribuir con inteligencia y comprometerse a tomar las medidas adecuadas al compartir la información. Los modelos de participación escalonada pueden equilibrar la equidad con la accesibilidad para las organizaciones más pequeñas.
- **Manejo y conservación de datos:** Los acuerdos de intercambio de información deben establecer requisitos claros sobre cuánto tiempo se conserva la inteligencia compartida, cómo se garantiza, quién puede acceder a ella y cuándo debe eliminarse.
- **Restricciones sobre el uso e intercambio posterior:** La inteligencia compartida debe utilizarse solo para la prevención del fraude y fines relacionados. El intercambio posterior solo debe permitirse con consentimiento explícito o dentro de la comunidad de intercambio definida.

- **Auditoría y rendición de cuentas:** Las organizaciones participantes deben mantener registros de la inteligencia recibida y las acciones tomadas, someterse a revisiones periódicas para verificar el cumplimiento e informar sobre los resultados totales para ayudar a los participantes a evaluar la eficacia de los esfuerzos.
- **Ciclos de retroalimentación:** Los destinatarios deben informar sobre las acciones tomadas en función de la inteligencia compartida y los resultados obtenidos.
- **Claridad de propósito:** Los acuerdos de intercambio de información deben definir explícitamente su objetivo operativo (p. ej., prevención del fraude, interdicción en curso, recuperación de activos, apoyo a procesos legales por un delito subyacente específico).

**Opciones del modelo de gobernanza:**

- **Bilateral/entre pares:** Este modelo se basa en relaciones de confianza simples y directas, pero tiene una escalabilidad limitada.
- **Consorcio:** Este enfoque proporciona un alcance y una detección de patrones más amplios, pero requiere una gobernanza más compleja.
- **Intermediario externo:** Esta opción aborda las preocupaciones competitivas, pero introduce dependencias operativas.

Las organizaciones deben seleccionar modelos basados en casos de uso específicos, relaciones existentes, dinámicas sectoriales y sensibilidades competitivas, en lugar de seguir un solo enfoque prescrito.

## Consideraciones principales y plan de acción

El grupo de trabajo debe priorizar la implementación práctica que permita a las organizaciones pasar de la intención al impacto sin requerir una transformación a gran escala y, luego, sentar las bases para lograr avances significativos en asociación con las organizaciones responsables en la atención de problemáticas de carácter estructural y de largo plazo necesarias para escalar de forma sostenida las iniciativas de combate al fraude.

### *Posibles acciones del grupo de trabajo*

1. **Desarrollar plantillas para acuerdos de intercambio de datos y plantillas de casos de uso** para tres a cinco escenarios de intercambio prioritario que documenten los elementos de datos exactos, la base legal, los requisitos de oportunidad, las protecciones, los requisitos de información contextual y las acciones habilitadas.
2. **Promover el intercambio inmediato de baja fricción** de alertas de tipología de fraude, identificadores hash, indicadores de infraestructura y patrones agregados.
3. **Desarrollar un kit de herramientas de datos sobre fraude y un manual de estrategias de intercambio de información** que asigne los elementos prioritarios de datos sobre fraude, su utilidad y fuente, mecanismos y vectores para intercambiar, y estándares existentes o necesarios para la interoperabilidad.
4. **Mapear las brechas en las aclaraciones legales y las disposiciones de puerto seguro** para el intercambio de información transfronteriza e intersectorial e involucrar a los legisladores para ayudar en los esfuerzos para abordarlas.

# Conclusión

El intercambio de inteligencia sobre fraude en el sector privado se puede lograr sin esperar nuevos marcos legales ni una transformación técnica a gran escala. El progreso depende de centrarse inicialmente en casos de uso de alto impacto con un valor operativo claro, elementos de datos específicos que las organizaciones puedan compartir de manera realista según los marcos legales existentes y modelos de gobernanza que generen confianza a través de la transparencia y la reciprocidad.

Las organizaciones deben comenzar inmediatamente con tipos de información de baja fricción y acuerdos bilaterales simples, y así crear capacidad operativa y confianza para escenarios de intercambio más complejos. Las recomendaciones del grupo de trabajo proporcionan una vía desde la fragmentación actual hacia un intercambio de inteligencia más sistemático, escalable y sostenible que ofrezca reducciones mensurables en las pérdidas por fraude.

# Acerca de ACAMS

ACAMS es una organización internacional líder dedicada a proporcionar oportunidades de formación, prácticas recomendadas y redes entre pares en materia de la AFC (del inglés anti-financial crime, prevención de los delitos financieros) a profesionales de todo el mundo. Con más de 110 000 miembros en más de 200 jurisdicciones y territorios, ACAMS se compromete con la misión de acabar con los delitos financieros mediante el intercambio de conocimientos sobre la prevención del lavado de dinero y el financiamiento al terrorismo y las sanciones, el liderazgo reflexivo, los servicios de mitigación de riesgos, las iniciativas ESG y las plataformas para el diálogo público-privado.

La certificación CAMS de la asociación es la calificación de referencia para los Especialistas en AFC, mientras que la certificación CGSS es su principal calificación especializada para los especialistas en sanciones. Los más de 60 capítulos de la ACAMS a nivel mundial amplifican aún más la misión de la asociación a través de iniciativas de formación y creación de redes.