GASA Capitulo México

Relatoria - 2ª Mesa Redonda

Fecha: 21 de julio de 2026 | **Duración:** 3 horas (10:00–13:00 h) | **Anfitriona:** Mastercard | **Asistencia:** Más de 35 participantes del sector financiero, bancario, telecomunicaciones, reguladores, plataformas digitales, fintech, gobierno, academia, medios y organismos internacionales | **Modalidad:** Sesión cerrada, Chatham House Rules

Este documento es una síntesis estructurada de las aportaciones realizadas durante la sesión. No representa las opiniones de ningún participante individual ni las recomendaciones finales del grupo o del capítulo GASA México.

1. INTRODUCCIÓN

El 21 de julio de 2026 se celebró en las instalaciones de Mastercard México la Segunda Mesa Redonda del Capítulo GASA México — segundo hito en la construcción de una respuesta coordinada frente a la crisis de fraude digital que afecta al país. Si la primera sesión (28 de enero de 2026, Scotiabank) tuvo como propósito establecer el diagnóstico compartido y construir la coalición, esta segunda mesa se planteó convertir ese diagnóstico en compromisos concretos y en una hoja de ruta operativa.

La sesión se organizó en dos etapas de debate: **la primera** abordó la pertinencia y urgencia de la convergencia entre la agenda de ciberseguridad y la agenda antifraude; **la segunda** abordó los componentes de comunicación, concienciación y campañas educativas. La sesión concluyó con la formulación de acciones concretas.

2. CONTEXTO: CONTINUIDAD DESDE LA PRIMERA MESA REDONDA

La apertura incluyó una síntesis de los resultados de enero para facilitar la incorporación de nuevos participantes.

Magnitud del problema identificada en la primera mesa:

- Pérdidas de 139,000 millones de pesos en 2025 por fraude y estafas digitales (Reporte GASA Estado de las Estafas en México 2025). (Link)
- El 59% de los adultos mexicanos fue víctima de fraude en el último año; el 76% afirma poder reconocer una estafa — paradoja que evidencia la sofisticación de la ingeniería social.
- El 79% de los intentos ocurre por canales de mensajería directa.
- A nivel global, solo el 0.05% de los ciberdelitos son perseguidos penalmente.

Tres obstáculos estructurales:

- **Brecha de coordinación:** los bancos tienen datos transaccionales, pero carecen del "músculo de las telcos" para completar investigaciones. Consenso de la primera mesa: "Tenemos que empezar a compartir la información."
- **Brecha jurídica:** los datos técnicos (IPs, registros de llamadas, movimientos bancarios) no tienen validez como evidencia ante el Ministerio Público. El 48% de las quejas ante CONDUSEF por fraude nunca llegan a una denuncia penal.
- **Brecha de liderazgo:** la estrategia antifraude se diseña sin acompañamiento técnico, replicando enfoques que en otros países no han dado resultados.

3. PLANTEAMIENTO ESTRATÉGICO: EL ARGUMENTO DE LA CONVERGENCIA

GASA México, presentó el argumento que estructuró los debates: la ciberseguridad en México ya no puede verse como un tema puramente técnico. El fraude digital, las estafas y la extorsión funcionan hoy como la infraestructura financiera y operativa de redes criminales más amplias, responsables también de lavado de

dinero, trata de personas y trabajo forzado. El delito financiero digital opera como una cadena industrializada de tres fases:

- **Iniciación:** captación mediante identidades sintéticas, webscraping y manipulación a escala (phishing, vishing, smishing hiperpersonalizado con IA).
- **Ejecución:** compromiso de dispositivos, clonación de voz, toma de cuenta, suplantación de identidad.
- **Extracción y lavado:** retiro vía cuentas mulas, cajeros y criptoactivos para salir de jurisdicciones locales antes de que los sistemas puedan rastrear los fondos.

El referente de Washington. - Se citó la Orden Ejecutiva de la Casa Blanca de marzo de 2026 *"Combating Cybercrime, Fraud, and Predatory Schemes against American Citizens"* como evidencia de que esta convergencia ya es una realidad en la política pública del principal socio comercial de México. La orden: (i) trata el fraude digital como asunto de seguridad nacional, no como delito financiero menor; (ii) no distingue entre cártel de droga y red criminal digital; y (iii) establece consecuencias diplomáticas —sanciones, restricciones de visa, límites a la asistencia exterior— para países que toleren esas redes. La conclusión formulada para orientar el debate: *"Estados Unidos ya convergió sus agendas. Ciberseguridad, antifraude, prevención de lavado y persecución del crimen organizado son, para Washington, una sola operación. México aún las trata como silos separados. Esa fragmentación nos expone a una presión diplomática creciente y a seguir perdiendo la batalla contra redes que ya tienen integrado lo que nosotros seguimos separando."*

4. PRIMERA ETAPA: CONVERGENCIA CIBERSEGURIDAD / ANTIFRAUDE

La fragmentación es interna y sectorial. El primer hallazgo del debate fue organizacional: la separación entre ciberseguridad y antifraude no existe solo entre sectores, sino al interior de las propias instituciones. Participantes del sector bancario describieron estructuras en las que ambas áreas operan de manera independiente, sin canales formales de comunicación, con políticas antispam y antispoofing definidas sin participación de las áreas de fraude. Se documentó que un mismo ataque atraviesa las competencias de tres áreas distintas —prevención de fraude, ciberseguridad e inteligencia— sin que ninguna tenga visión completa del ciclo. La integración de una tercera función, la prevención de lavado de dinero, fue identificada como condición necesaria para que el modelo sea completo: las tres áreas trabajan con información que en muchos casos es la misma, sin compartirla.

El dato de Mastercard. (Mastercard) presentó el dato empírico más influyente de la sesión: a nivel global, el 70% de las transacciones que terminan en fraude confirmado inician con una brecha del lado de los equipos de ciberseguridad. Este dato invierte la lógica convencional y demuestra que las dos agendas están causalmente conectadas.

La perspectiva regulatoria. Participantes representando al regulador de telecomunicaciones plantearon la necesidad de distinguir entre spam, estafas, fraudes y extorsión, dado que el marco normativo aplicable a cada categoría es distinto. Se señaló que aplicaciones de mensajería como WhatsApp —canal del 78% de los intentos de fraude— no están sujetas a la regulación de telecomunicaciones, mientras que llamadas y SMS sí lo están. Se identificó que la numeración, el código corto y el nombre del remitente en SMS son recursos del Estado hoy explotados para el fraude sin regulación suficiente.

La dimensión de seguridad nacional. Especialistas plantearon que los parámetros jurídicos deben transitar de un enfoque de seguridad pública a uno de seguridad nacional, lo que modificaría las condiciones legales para compartir información. Se identificó la necesidad de involucrar a organismos de inteligencia —CNI, Fiscalía, Unidad de Inteligencia Financiera— en el proceso. Participantes de gobierno documentaron que los bloqueos para el intercambio de información son también de carácter político, no solo técnico o legal: las resistencias institucionales a compartir datos constituyen un obstáculo tan real como las limitaciones normativas.

La paradoja técnica. La síntesis técnica del debate reveló la paradoja central: la información ya existe, pero no se comparte. Las áreas de ciberseguridad, antifraude y prevención de lavado utilizan frecuentemente los mismos datos sin comunicarlos entre sí, produciendo puntos ciegos que el crimen sí tiene resueltos. La solución requiere,

además de tecnología, la institucionalización de los mecanismos de coordinación; sin formalización legal, las acciones quedan expuestas a impugnaciones.

5. SEGUNDA ETAPA: CONCIENCIACIÓN, COMUNICACIÓN Y CAMPAÑAS

La segunda etapa partió de una premisa compartida: las estrategias basadas únicamente en información están caducas frente a ataques que explotan los mecanismos psicológicos de la decisión. El dato que lo ilustra es contundente: el 76% de los mexicanos cree poder detectar una estafa, pero el 59% ha sido víctima de una.

- **Campañas gremiales.** Se planteó la campaña coordinada entre instituciones —bajo el paraguas de GASA México— como la acción de implementación más rápida disponible. El problema central identificado fue la falta de armonización de mensajes: cuando cada actor comunica de manera distinta, los mensajes se cancelan entre sí y el ciudadano queda sin una referencia clara de comportamiento seguro.

- **Diseño conductual.** GASA planteó que el objetivo no debe ser informar en abstracto, sino introducir fricción en el momento de la operación: una pausa deliberada que active el pensamiento analítico antes de que el ciudadano tome la decisión que el defraudador quiere que tome. Los defraudadores activan deliberadamente el Sistema 1 de decisión —rápido, emocional, automático— mediante tres mecanismos: ambición, miedo y altruismo. Las campañas deben diseñarse para activar el Sistema 2 —analítico, deliberado— en el momento crítico, con formatos específicos para WhatsApp, YouTube y SMS, e incorporando la práctica del simulacro preventivo.

- **Vocería y segmentación.** Se acordó abandonar la lógica de campaña única en favor de mensajes segmentados por perfil de víctima. La vocería bajo el paraguas de GASA México y UNODC —cuya alianza formal data de marzo de 2026— fue identificada como estratégicamente superior a la de cualquier actor individual, por su neutralidad y credibilidad transectorial.

6. CONCLUSIONES Y ACCIONES

El debate de julio reveló que la convergencia entre ciberseguridad y antifraude no es un argumento académico: es el reflejo de cómo opera la amenaza en la realidad. Los defraudadores no distinguen entre "infraestructura" y "cliente"; esa frontera la disolvieron hace tiempo. La respuesta institucional no puede seguir honrando una distinción que la amenaza ya superó.

- La convergencia ciberseguridad-antifraude es un imperativo operativo: el 70% de los fraudes confirmados inicia con una brecha de ciberseguridad; un mismo ataque atraviesa tres áreas sin que ninguna tenga visión completa.
- La fragmentación es interna y externa, y requiere atención simultánea en ambas dimensiones.
- México opera bajo presión diplomática creciente: la Orden Ejecutiva de Washington establece consecuencias para países que toleren las redes del ciberfraude; la convergencia de agendas es también una condición de gestión bilateral.
- La comunicación efectiva requiere diseño conductual, segmentación y presencia en los canales donde el fraude ocurre.
- La neutralidad de GASA México y UNODC es un activo estratégico para articular mensajes y acciones que ningún actor sectorial puede producir con la misma credibilidad.

Acciones acordadas:

- **Anatomía sistémica del fraude en México:** documentar actores y fases del ciclo completo (iniciación, ejecución, extracción), coordinado por GASA México con apoyo de UNODC.
- **Campañas perfiladas y multicanal:** mensajes segmentados por perfil de víctima, con base en diseño conductual, usando los canales ofrecidos por los participantes, bajo la vocería de GASA México y UNODC.

- **Incorporación al debate sobre la Ley General de Ciberseguridad:** la necesidad de convergencia entre fraude y ciberseguridad debe quedar reflejada en las propuestas de ley que actualmente lidera la ATDT.

"Nuestra misión es sensibilizar a los ciudadanos y a los responsables de la toma de decisiones sobre la necesidad fundamental de armonizar las estrategias de ciberseguridad y de lucha contra el fraude, reconociendo que su éxito está íntimamente ligado. Solo una auténtica colaboración multisectorial entre los sectores público y privado, podremos desarrollar la capacidad colectiva necesaria para proteger a nuestra sociedad frente a las amenazas digitales en constante evolución."

Sissi De La Peña
Directora — Capítulo México, Global Anti-Scam Alliance