GASA
Global Anti-Scam Alliance

Relatoría de la 1ra Mesa Redonda del GASA México

INTRODUCCIÓN

El 28 de enero de 2026, en las instalaciones de Scotiabank en la Ciudad de México, se llevó a cabo la Primera Mesa de Debate del capítulo GASA México, un hito fundacional en la construcción de una respuesta coordinada frente a la crisis de fraude digital que afecta al país. GASA México — capítulo nacional de la Global Anti-Scam Alliance — nace con el propósito de catalizar la colaboración multisectorial para enfrentar pérdidas económicas que ascienden a 139 mil millones de pesos (según el reporte *Estado de las Estafas en México 2025* de GASA) y contrarrestar la creciente sofisticación de ataques impulsados por inteligencia artificial.

El objetivo central de esta primera sesión fue establecer los fundamentos de una agenda nacional integral que unifique esfuerzos entre el sector financiero, las plataformas digitales, las telecomunicaciones, el gobierno y la sociedad civil para romper los silos institucionales y crear sistemas de respuesta coordinada.

A la mesa de debate asistieron representantes del sector financiero (Scotiabank, Banorte, BBVA, Banamex y Clip), del ecosistema digital (Microsoft, TikTok, Google, Mercado Libre y Tools for Humanity), del sector telecomunicaciones (Telefónica y AT&T), de gobierno y reguladores (la Secretaría de Relaciones Exteriores, la CNBV y la Comisión Reguladora de Telecomunicaciones), del Poder Legislativo (las Comisiones de Inteligencia Artificial del Senado y de Ciencia y Tecnología de la Cámara de Diputados), así como empresas especializadas en prevención de fraude (Mastercard, Nasdaq Verafin, Feedzai y VoiSek) y organizaciones de sociedad civil como TechCheck. Cabe destacar que durante este encuentro se formalizó la firma del Memorándum de Entendimiento entre GASA México y la Dirección General de Ciberseguridad de la Agencia de Transformación Digital y Telecomunicaciones (ATDT) del Gobierno de México, mediante el cual esta última se integra como miembro del Board de GASA México para sumar esfuerzos en la lucha nacional contra las estafas y el fraude en línea.

El presente documento sirve como una síntesis estructurada de las aportaciones, diagnósticos y propuestas planteadas por los participantes durante la sesión del 28 de enero, con el fin de articular una visión compartida que oriente los trabajos futuros de la coalición. Contiene ejemplos de lo que dicho trabajo podría implicar; no representa las opiniones de ningún participante individual de la mesa redonda ni las recomendaciones finales del grupo ni del capítulo GASA México.

GASA
Global Anti-Scam Alliance

CONTEXTO ESTRATÉGICO – ¿PORQUE DEBEMOS ACTUAR?

México se encuentra en una coyuntura crítica que exige una transición inmediata del modelo de seguridad reactiva hacia uno de **"corresponsabilidad activa"**. Al compartir con Brasil la posición como el mercado más atractivo y vulnerable para el cibercrimen en América Latina, el país no puede permitirse respuestas aisladas.

El fraude digital opera mediante redes criminales transnacionales altamente coordinadas; por lo tanto, la defensa debe ser sistémica. La corresponsabilidad activa no es opcional: es el único paradigma capaz de articular a los sectores financiero, tecnológico y gubernamental en un frente unificado contra ataques que se ejecutan en milisegundos.

La urgencia de actuar se manifiesta en la explosión de la superficie de ataque. México ha transitado de 600,000 comercios digitales en 2014 a más de 6 millones en la actualidad. Este crecimiento no es solo un éxito de inclusión financiera, sino que representa la creación de una "alternativa digital al efectivo" que ha superado las capacidades de supervisión institucional. Esta expansión masiva ha degradado la confianza sistémica, permitiendo que el anonimato digital sea explotado como un vector de impunidad.

De acuerdo con los hallazgos del *Microsoft Digital Defense Report* y datos del primer semestre de 2025, la magnitud de la amenaza es asimétrica:

- **Volumen masivo de ataques:** Solo en los servicios de correo de Microsoft, se registraron 15.9 mil millones de intentos de ataque durante la primera mitad de 2025.
- **Automatización hostil:** Se bloquean sistemáticamente 1.6 millones de intentos de creación de cuentas falsas por hora a nivel global.
- **Sofisticación regional y bots:** En el primer semestre de 2025, más del 90% de las solicitudes de nuevas cuentas fueron generadas por bots maliciosos. México y Brasil concentran a los actores más avanzados de la región, quienes utilizan IA para perfeccionar deepfakes y suplantación de identidad.

Esta escala exige un diagnóstico técnico que resuelva la fragmentación actual antes de que la desconfianza del usuario colapse el ecosistema digital.

GASA
Global Anti-Scam Alliance

DIAGNÓSTICO DE LA FRAGMENTACIÓN INSTITUCIONAL Y OPERATIVA

El principal obstáculo para la seguridad nacional digital es el desfase entre la detección técnica y la respuesta judicial. Actualmente, existe un cuello de botella crítico en la "legalización de la información" dentro de la carpeta de investigación. Mientras los bancos y telcos pueden identificar un fraude en tiempo real, los protocolos para convertir esos datos técnicos (IPs, registros de llamadas, movimientos bancarios) en evidencia válida ante un tribunal son obsoletos, lo que rompe la cadena de justicia.

La fragmentación jurisdiccional garantiza la impunidad. El modelo actual de los Ministerios Públicos (MP), limitado por fronteras físicas, fracasa ante el delito digital: un fraude iniciado en la Ciudad de México con depósitos en Cancún o mediante criptomonedas minadas en jurisdicciones internacionales (como India o Brasil) deja a la autoridad local sin competencia operativa. Esta desconexión institucional genera una **"fragmentación de la confianza"** donde el usuario, además de ser defraudado, sufre el "bullying" burocrático de un sistema que lo revictimiza, resultando en que el 48% de las quejas en CONDUSEF por cargos no reconocidos nunca lleguen a una denuncia penal.

Operación en Red de la Ciberdelincuencia	**Respuesta en Silos de las Instituciones**
Colaboración global y compartición de tácticas en tiempo real entre criminales.	Fragmentación de la información; bancos y telcos no comparten datos de origen de forma ágil.
Uso de IA para automatizar ataques masivos y evadir controles de identidad.	Procesos legales manuales; falta de protocolos para la "legalización" de evidencia digital.
Explotación de vacíos jurisdiccionales y fronteras territoriales.	Ministerios Públicos limitados por competencias estatales y burocracia territorial.
Agilidad extrema para mutar vectores de ataque.	Marcos regulatorios estáticos y falta de capacitación técnica en tomadores de decisión.

GASA
Global Anti-Scam Alliance

LOS CUATRO PILARES DEL ESCUDO NACIONAL (MARCO LEGISLATIVO)

Desde la Comisión de IA en el Senado de la República, y tras 72 conversatorios y más de 280 intervenciones especializadas en 2025, se ha definido la arquitectura para una propuesta de la Ley General para el Fomento y Regulación de la IA. Este marco legal sugiere pasar de identificar a la Inteligencia Artificial como una amenaza a identificar su capacidad estratégica de defensa nacional, equilibrando la productividad con la mitigación de riesgos sistémicos. En el contexto de esta mesa redonda, el marco ofreció cuatro pilares relevantes para organizar las ideas sugeridas para acciones legislativas que ayuden a contrarrestar el aumento del fraude y las estafas en línea.

1. Pilar Punitivo: Se plantea actualizar los tipos penales para eliminar el anonimato como escudo. La propuesta de legislación busca garantizar que los delitos cometidos mediante tecnologías emergentes sean sancionados con la misma severidad que los físicos, así como el fortalecimiento de capacidades federales.

2. Pilar de Detección: Plantea la implementacion de mecanismos de colaboración técnica para identificar engaños en tiempo real. Implica la creación de una infraestructura de "señales compartidas" donde la detección de un bot o una suplantación por parte de una plataforma digital active alertas inmediatas en el sector bancario.

3. Pilar Predictivo: Este pilar es el eje de la inhibición proactiva. Se fundamenta en la regulación de la Comisión Nacional Bancaria y de Valores (CNBV) **publicada en junio de 2024**, la cual es **obligatoria desde enero de 2025**. Esta normativa establece que las instituciones financieras implementen sistemas de análisis de comportamiento transaccional basados en IA para bloquear movimientos que superen límites habituales o presenten patrones atípicos antes de que el capital salga del sistema.

4. Pilar Preventivo (Cultura de Prevención): La prevención busca dejar de ser un concepto educativo para el usuario final y convertirse en un mandato de capacitación para tomadores de decisión y autoridades. El éxito del escudo depende de que los legisladores, jueces y directivos comprendan la ingeniería social y los riesgos digitales para romper los paradigmas que limitan la respuesta institucional.

GASA
Global Anti-Scam Alliance

MATRIZ DE RESPONSABILIDADES PARA UNA COORDINACIÓN INSTITUCIONAL EFECTIVA

La seguridad digital es un activo compartido. Los asistentes coincidieron en que México exige a cada actor cerrar vectores de ataque específicos mediante compromisos técnicos medibles. Estos son algunos ejemplos de los tipos de compromisos que se recomendaron:

1. Sector Bancario: Debe liderar la implementación de límites transaccionales habitacionales y sistemas antifraude robustos. Nota de Riesgo Estratégico: La ausencia de la Asociación de Bancos de México (ABM) en los diálogos legislativos iniciales representa un vacío de coordinación que se debe rectificar mediante la integración a las mesas de GASA.

2. Telecomunicaciones: El enfoque prioritario debe ser el control de Agregadores y Call Centers, quienes gestionan los recursos de numeración utilizados para las estafas. Es imperativo visibilizar el riesgo en protocolos de mensajería como **I2P**, un vector de ataque crítico que anonimiza el tráfico y crea puntos ciegos para los operadores tradicionales.

3. Plataformas Digitales: Plataformas Digitales podrian intensificar el combate a bots. Un componente esencial es la capa de "Proof of Personhood" (Prueba de Humanidad), para diferenciar humanos de IA y mitigar el impacto de los deepfakes en la verificación de identidad.

4. Gobierno y reguladores: La CNBV, la Secretaría de Seguridad y la Cancillería podrían armonizar la gobernanza global. México debería utilizar su posición en la Convención de la ONU contra el Ciberdelito para facilitar la persecución transfronteriza y la recuperación de activos.

GASA
Global Anti-Scam Alliance

HOJA DE RUTA: IMPLEMENTACIÓN Y "QUICK WINS"

Para recuperar la confianza del consumidor y romper el ciclo de impunidad, se sugiere identificar un plan nacional o desarrollar una agendad de política pública Antifraude-anti estafas en donde organizaciones como GASA México podrían apoyar a orquestas acciones específicas dentro del ecosistema.

Hitos de Implementación (Check-list):

- ☐ **Alineación Global (Marzo 2025):** Participación estratégica en el Fraud Summit de Viena para integrar estándares internacionales de la ONU e Interpol.
- ☐ **Victoria Temprana**: Establecer el protocolo de compartición de datos entre bancos y telcos para rastrear el origen de llamadas y mensajes de fraude sin esperar ciclos legislativos largos.
- ☐ **Restauración de Confianza:** Documentación y difusión masiva de casos de éxito de recuperación de activos, demostrando que la denuncia coordinada produce detenciones y devoluciones de fondos.

CONCLUSIÓN: HACIA UNA CULTURA DE PREVENCIÓN NACIONAL

El éxito de las acciones especificas y/o la ruta que se decida no se medirá por la sofisticación de su tecnología, sino por la restauración de la **confianza en el sistema financiero y digital**. Con un 48% de quejas ante CONDUSEF relacionadas con fraude, el costo de la inacción es la erosión de la economía digital. La tecnología y la criptografía son herramientas esenciales, pero la base de un escudo sólido es una **Cultura de la Prevención** que permee desde la alta dirección gubernamental hasta el ciudadano.

México debe dejar de ser un mercado apetitoso para el delincuente y transformarse en una jurisdicción de alta resistencia mediante la corresponsabilidad activa.

> "La visión es establecer un verdadero dialogo multisectorial y una ruta de trabajo nacional que apunte a identificar una agenda contra las estafas, los fraudes y los engaños digitales. Esta debe ser una estrategia multi-actor donde la principal capacidad reside en la suma de esfuerzos del sector público y privado para proteger al ciudadano."

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