Número 112 | Marzo 2026

NTT DATA

Radar

El magazine de ciberseguridad

Romper la cadena del fraude: el papel clave de las mulas financieras

Por Miguel Angel Soler Barba y Alejandra Romero Gutiérrez

El fraude financiero se ha convertido en uno de los grandes desafíos globales de nuestro tiempo. Su crecimiento sostenido no entiende de fronteras: afecta a bancos, empresas, comercios, instituciones públicas y ciudadanos de todos los continentes. Estafas de inversión cada vez más sofisticadas, suplantaciones masivas de identidad, fraudes de pago y ataques de ingeniería social se combinan hoy con un ecosistema criminal que opera a escala internacional. En este escenario, hay un elemento común que sigue siendo decisivo para el éxito de los delincuentes: las mulas financieras.

Las mulas —personas que mueven fondos ilícitos a través de sus cuentas, a veces engañadas y otras actuando voluntariamente— se han convertido en la infraestructura esencial del fraude moderno. Sin ellas, los defraudadores no podrían convertir sus ganancias en dinero utilizable ni ocultar su rastro a través de múltiples movimientos de fondos y de distintas jurisdicciones. La naturaleza global del sistema financiero digitalizado ha multiplicado tanto las oportunidades como los riesgos, haciendo que la lucha contra las mulas sea un desafío transnacional.

El panorama regulatorio avanza para responder a esta amenaza. Organismos internacionales como el GAFI/FATF, nuevas autoridades europeas como AMLA, y marcos como PSD2/PSR, DORA, NIS2, el futuro estándar global de pagos instantáneos o el Digital Euro Package están imponiendo requisitos más estrictos en materia de verificación de identidad, monitorización de transacciones y gestión del riesgo operativo y cibernético. La regulación ya no se centra únicamente en cumplir procedimientos, sino en demostrar efectividad real en la prevención del fraude, incluida la detección y desarticulación de redes de mulas.

La ciberseguridad, por su parte, se ha convertido en un pilar inseparable de la lucha contra el fraude. Los ataques actuales combinan *malware*, *phishing*, *spoofing*, secuestro de sesiones y manipulación psicológica a gran escala. La colaboración entre los equipos de fraude y los centros de operaciones de seguridad (SOC) es ahora imprescindible para correlacionar indicios técnicos y financieros a través de las ciber inteligencia. Las mulas son el destino final de muchos de estos ataques, por lo que el eslabón entre ciber amenazas y fraude transaccional se ha estrechado como nunca.

La complejidad y velocidad de las redes de muleros hacen inviable una respuesta basada únicamente en reglas estáticas o revisiones manuales. La analítica avanzada, en sus distintos niveles de madurez, se ha convertido en el principal aliado para anticipar, detectar y desarticular estas redes.

A través de cuadros de mando y análisis exploratorios, las organizaciones pueden identificar tipologías de fraude, concentraciones por canal o producto y analizar el ciclo de vida de las cuentas mula. Los modelos estadísticos y de *machine learning* permiten estimar la probabilidad de que una cuenta actúe como mulera, así como detectar comportamientos anómalos y analizar patrones de red.

Y la combinación de *scores* de riesgo, reglas dinámicas y simulaciones está permitiendo a las organizaciones recomendar acciones óptimas, priorizar investigaciones y equilibrar fraude, coste y experiencia de cliente. Todo lo anterior hace necesario un aprendizaje continuo y ahí es donde interviene la IA (aprendiendo de forma continua, detectando señales débiles y combinaciones complejas invisibles para reglas tradicionales, analizando redes completas y escalando la detección a millones de transacciones y relaciones).

Si a esto le sumamos la IA generativa, esto introduce un cambio cualitativo en la lucha contra los muleros, al centrarse en amplificar la capacidad de los equipos humanos.

Y el horizonte tecnológico va aún más lejos. La computación cuántica, aunque hoy todavía es incipiente, plantea retos y oportunidades: por un lado, podría comprometer en el futuro los métodos actuales de cifrado; por otro, promete capacidades analíticas sin precedentes para rastrear relaciones complejas entre miles de cuentas y transacciones. Prepararse para un mundo “post-cuántico” será esencial para mantener la resiliencia del ecosistema financiero.

Desde una perspectiva estratégica, esta realidad pone de manifiesto un mensaje clave para el sector: sin una visión integral e integrada del fraude en general y del fenómeno de las mulas en particular no habrá una prevención eficaz. Las redes de mulas evolucionan con rapidez, adaptándose a los controles existentes, y solo pueden ser contenidas mediante unas operaciones ágiles, un control férreo y unas capacidades analíticas capaces de aprender, anticipar y ajustarse de forma continua.

La lucha contra las mulas deja de ser un problema puramente operativo para convertirse en una decisión estructural sobre cómo se gobierna el riesgo en la era digital.

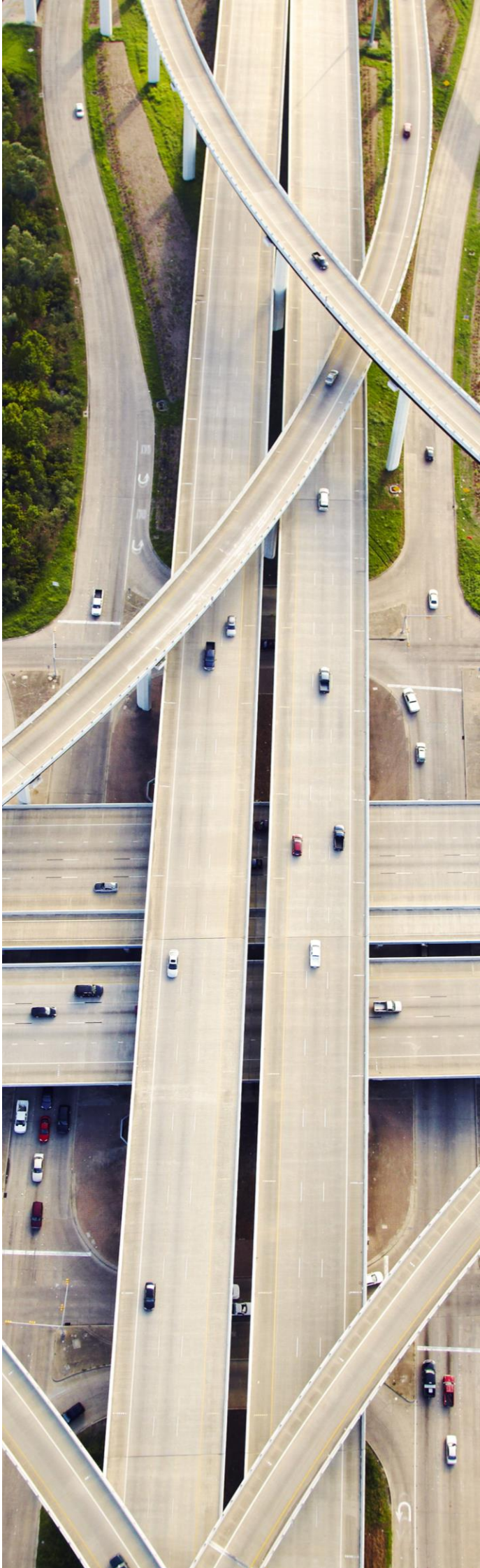
En definitiva, la problemática de las mulas financieras es mucho más que un asunto operativo: es un desafío global que requiere regulación inteligente (pero que no limite la actuación razonable del ciudadano), tecnología que aúne fraude y ciberseguridad, analítica avanzada y colaboración transfronteriza. Si somos capaces de debilitar este eslabón crítico, podremos reducir significativamente el fraude y proteger la confianza que sostiene al sistema financiero mundial.

A lo largo de este ejemplar de nuestra publicación Radar, profundizaremos en cómo las entidades financieras gestionan la detección y mitigación de cuentas mula a lo largo de su ciclo de vida. El proceso se divide en tres etapas críticas: el alta del cliente, el periodo de latencia y el análisis de la transaccionalidad en tiempo real. Se destacará la evolución tecnológica mediante el uso de modelos de aprendizaje automático proactivos y reactivos que permiten identificar patrones sospechosos con mayor precisión.

Además, se analizará cómo las herramientas de inteligencia artificial facilitan tanto la creación de identidades falsas por parte de criminales como su detección por parte del banco. Finalmente, el documento reflexionará sobre la futura implementación de sistemas de agentes para automatizar el análisis de alertas y mejorar la eficiencia operativa.

Miguel Angel Soler Barba
Responsable FinCrime

Alejandra Romero Gutiérrez
Responsable Prevención de Fraude



Ataques a instituciones europeas

Cibercrónica por Leire Cubo Arce

Los primeros meses de 2026 han confirmado que el escenario de ciberseguridad continúa tensionado y en evolución constante. Durante el último mes, se han registrado incidentes relevantes que afectan a instituciones públicas europeas, grandes eventos internacionales y sectores estratégicos, al tiempo que los informes consolidados reflejan un crecimiento sostenido de *ransomware* y fraude digital.

Uno de los episodios más significativos se produjo en el ámbito institucional europeo. La Comisión Europea confirmó a finales de enero un acceso no autorizado a su plataforma de gestión de dispositivos móviles corporativos (MDM). El incidente, detectado y contenido en menos de nueve horas, permitió a los atacantes acceder a datos personales limitados de algunos funcionarios, entre ellos nombres y números de teléfono profesionales.

Aunque no se comprometieron directamente los dispositivos móviles gestionados por la plataforma, las autoridades advirtieron del riesgo de que la información extraída pudiera utilizarse en campañas de *phishing* altamente dirigidas contra personal institucional. El caso vuelve a poner el foco en la exposición de herramientas críticas de gestión interna, cada vez más atractivas para actores avanzados.

En paralelo, el contexto geopolítico volvió a trasladarse al ciberespacio. En las semanas previas a los Juegos Olímpicos de Invierno en Italia, la agencia nacional de ciberseguridad italiana confirmó intentos coordinados de ataques de denegación de servicio (DDoS) contra portales oficiales del evento y contra infraestructuras vinculadas al entorno turístico y logístico en Cortina d'Ampezzo.

Las acciones, atribuidas a un grupo hacktivista pro-ruso, buscaban generar interrupciones y visibilidad mediática en un evento de alto perfil internacional. Las medidas de mitigación desplegadas lograron neutralizar el tráfico malicioso sin que se produjeran caídas significativas de servicios, pero el episodio confirma que los grandes acontecimientos globales continúan siendo objetivos simbólicos dentro de la confrontación digital.

En el ámbito nacional, los datos más recientes reflejan un aumento considerable de la actividad delictiva. El Instituto Nacional de Ciberseguridad (Incibe) informó de que durante 2025 se gestionaron más de 122.000 incidentes, lo que supone un incremento del 26 % respecto al año anterior. Destaca especialmente el crecimiento del 171 % en los casos de robo de información digital, así como la persistencia de miles de campañas de *phishing* y fraude online. Además, más de 400 incidentes afectaron a operadores considerados esenciales, incluyendo sectores como banca, transporte y energía. Estas cifras evidencian que la amenaza no solo es más frecuente, sino que impacta directamente en infraestructuras críticas y de servicios estratégicos.

El *ransomware*, por su parte, mantiene una tendencia elevada a nivel global. Informes sectoriales correspondientes a enero de 2026 muestran un volumen de ataques superior a la media histórica, con especial incidencia en organizaciones del ámbito sanitario, gubernamental e industrial. Los grupos criminales continúan perfeccionando modelos de doble extorsión, combinando cifrado de sistemas con la amenaza de publicación de datos exfiltrados. La profesionalización de estas estructuras delictivas y la diversificación de sus vectores de acceso —frecuentemente a través de credenciales comprometidas o vulnerabilidades en servicios expuestos— complican la contención temprana de los ataques.

Al mismo tiempo, los expertos han alertado sobre la explotación masiva de dispositivos domésticos conectados, especialmente televisores inteligentes y sistemas de *streaming* basados en Android. Estos equipos, a menudo mal configurados o sin actualizaciones de seguridad, están siendo reclutados para formar parte de *botnets* utilizadas en ataques distribuidos de denegación de servicio. La tendencia demuestra que la superficie de ataque ya no se limita al perímetro corporativo tradicional, sino que se extiende al ecosistema digital del hogar conectado, que puede convertirse sin saberlo en infraestructura al servicio del atacante.

En conjunto, el último mes dibuja un escenario en el que la actividad cibercriminal combina motivaciones políticas, lucro económico y explotación sistemática de vulnerabilidades técnicas. La rapidez en la detección, la capacidad de respuesta coordinada y la gestión del ciclo de vida tecnológico se consolidan como elementos clave para reducir el impacto. El inicio de 2026 confirma así que la ciberseguridad continúa siendo un componente estratégico esencial para la estabilidad institucional, económica y social en un entorno cada vez más interconectado.

Leire Cubo Arce
Cybersecurity Engineer

Mulas financieras: reconsiderando la relación entre el AML y el fraude

Artículo por José Frías Hernando

En la última década, casi todos los aspectos de la actividad financiera han cambiado de la noche a la mañana. Los clientes operan dentro y fuera de los canales digitales con una facilidad que hace años parecía imposible, y las organizaciones han tenido que adaptar su modelo a una relación mucho más en línea. Pero en medio de esta transformación ha surgido un compañero incómodo: el crimen financiero también ha cambiado. Ha estado haciendo esto silenciosamente, explotando brechas en el sistema y, en muchos casos, actuando más rápido que los controles que ya existen.

A esta realidad se suma una asimetría fundamental: mientras las entidades financieras operan bajo marcos regulatorios cada vez más exigentes —cumpliendo con obligaciones en materia de AML (Anti-money-Laundering), protección al consumidor, privacidad, gobernanza y resiliencia operativa—, los ciberdelincuentes no están sujetos a ninguna de estas restricciones. No deben equilibrar innovación con cumplimiento, ni velocidad con control; esa ausencia de obligaciones les otorga una agilidad que, en la práctica, se traduce en una ventaja estructural frente a organizaciones que sí deben proteger a sus clientes sin dejar de cumplir la regulación.

Pero uno de los cambios que esta nueva realidad ha introducido es de mayor preocupación para los supervisores: las mulas financieras están creciendo, diversificándose. Durante mucho tiempo, el sector asumió que una mula encajaba en el modelo clásico del individuo que prestaba su cuenta y recibía alguna remuneración financiera o un buen retorno. Un actor de buena voluntad, casi siempre consciente de su participación. Hoy en día, esa caricatura no se aplica.

Las entidades se encuentran con estudiantes atraídos por ofertas que, aparentemente, parecen inocentes, trabajadores que demandan ingresos adicionales sin ser conscientes de que están siendo explotados, víctimas de suplantación, pero, cada vez más, identidades sintéticas que evaden los controles iniciales mediante técnicas cada vez más sofisticadas.

Este escenario no solo complica la detección, sino que también cambia el panorama de la percepción del riesgo y obliga a cuestionar cómo se caracteriza y se establece la protección desde el inicio de la relación con el cliente.

Un problema que se ha movido al centro de la agenda regulatoria

Este fenómeno no es nuevo, el regulador lo tenía incluido en su hoja de ruta mucho antes de que llegara a los titulares de la prensa. El tema de las mulas no es anecdótico para las autoridades de supervisión.

También lo llaman un síntoma: cuando una entidad permite que sus productos sean utilizados para mover dinero sucio, incluso cuando su cliente ha sido engañado, puede resaltar debilidades en sus políticas de acreditación, su capacidad para realizar revisiones analíticas regulares o la integridad de sus modelos de riesgo.

Con el tiempo, los supervisores han aumentado las exigencias. La verificación de identidad y los registros ya no son suficientes para satisfacerlos. Quieren saber tanto como sea posible sobre lo que hace la entidad para saber si el comportamiento del cliente es consistente con su perfil, si hay inconsistencias en sus actividades iniciales, si está sujeto a prácticas de manipulación o si está en patrones que ya están conectados a redes criminales.

Por lo tanto, la incorporación ya no es una fase de validación, sino que se convierte en una primera línea de defensa para establecer la calidad del crecimiento de la entidad.

Otra alteración importante tiene que ver con la responsabilidad. Es evidente que la mula puede ser potencialmente una víctima, sin embargo, el regulador no evalúa que esto sea un escudo para la entidad en su conjunto.

La expectativa es evidente: el banco necesitará demostrar que existe un diseño de control lo suficientemente robusto como para identificar efectivamente comportamientos anormales antes de que se conviertan en un riesgo operativo o reputacional.

AML y fraude: dos mundos que siempre estuvieron conectados, pero ahora deben unirse formalmente

Si algo ha favorecido el ascenso de las mulas es la distancia operativa entre los equipos de prevención del lavado de dinero y los equipos de fraude que, al menos durante años, ha existido. Ambos observaban señales complementarias, pero rara vez las incorporaban en una visión única.

AML miraba los flujos, la coherencia de los ingresos, el origen de los fondos. El fraude evalúa operaciones (incluyendo salida de fondos): dispositivos, patrones de acceso, tasa de transacciones y despliegue. Cada sitio generaba alertas por su propia lógica, no creando una historia completa sobre el cliente. Esta forma de hacer las cosas ya no se puede mantener. Las mulas cruzan exactamente un umbral entre los dos mundos, y si las piezas no están todas conectadas, el riesgo escapa a la detección.

Los más proactivos han encontrado esto; aquellos que están respondiendo entienden y abogan por que AML y fraude operen juntos y creen modelos compartidos, compartiendo datos, criterios y decisiones. Esto implica transformar la gobernanza, pero también los flujos de trabajo: casos unificados, análisis comunes, puntuación que integra perspectivas y, sobre todo, una lectura del comportamiento del cliente, no solo referido o mirando lo que hace el cliente, sino también la forma en que lo hace y la aparente intención de por qué lo hace.

El resultado es una imagen más amplia. En lugar de interpretar señales desconectadas, el establecimiento ve al cliente como una entidad completa en evolución y puede moverse antes para tomar medidas con implicaciones de mayor alcance.

El papel del negocio: crecimiento, sí, pero con una comprensión diferente del riesgo. El espacio empresarial está profundamente afectado por todos estos movimientos regulatorios y operativos. La adquisición de clientes ya no puede evaluarse por números. El volumen ya no es suficiente.

Ahora se busca lo que muchas instituciones están comenzando a llamar "crecimiento limpio": crecimiento en el que el comportamiento no se desgasta, que no produce alertas excesivas y que no se convierte en un factor de riesgo para la organización.

Porque cuando el crecimiento ignora esta dimensión del riesgo, el impacto no se limita a métricas internas o regulatorias: se traduce en clientes que se sienten desprotegidos, que aun sin sufrir una pérdida económica directa reducen su confianza, limitan su vinculación con la entidad y erosionan oportunidades clave de fidelización y *cross-selling*.

El primer resultado de esta mentalidad son los cambios en la política de admisión. Las entidades están incorporando filtros menos visibles, pero más relevantes, basados en indicadores tempranos de riesgo tanto de AML como de fraude.

No significa endurecer el proceso, sino aplicar más flexibilidad en ausencia de riesgo y más profundidad en los casos donde la evidencia indica la existencia de vulnerabilidad o exposición a la manipulación.

La adaptación del negocio: políticas cambiantes, *journeys* conscientes y un nuevo equilibrio entre crecimiento y calidad

Al mismo tiempo, los *journeys* del cliente están siendo rediseñados. Ya no se entienden como caminos lineales diseñados para maximizar la conversión. Y se están comenzando a integrar puntos de control más sofisticados, mensajes preventivos y, en algunos casos, restricciones dinámicas que se activan cuando el comportamiento del cliente se aleja de lo esperado.

Lejos de comprometer la experiencia del usuario, esta estrategia fomenta un entorno digital más seguro con una mayor conciencia de los peligros emergentes.

Las señales internas también están en movimiento. La conversión se convierte en conversión calificada; el valor del cliente se valora utilizando cosas que ni siquiera se tenían en cuenta hace unos años. Incluso los incentivos comerciales están comenzando a cambiar para incentivar un crecimiento que ya no recompensará segmentos de negocio que, a largo plazo, resultan en una mayor fricción operativa y una mayor exposición regulatoria.

Conclusión: un reto que redefine lo que significa hacer negocio en el sector financiero

Las mulas financieras no son una moda o una rareza estadística. Representan un crimen financiero que ha crecido en complejidad y aprovecha las vulnerabilidades en el sistema subyacente.

Su enorme escala ha obligado al sector a acelerar los cambios necesarios que han estado en proceso durante un tiempo: más armonización de las prácticas de AML y fraude; políticas flexibles; caminos más deliberados; una mentalidad de riesgo que observa a sus clientes a medida que avanzan en su ciclo de vida.

El regulador marcó el camino, pero son las propias organizaciones las que deben ver cómo el crecimiento sostenible depende de cómo pueden detectar esta amenaza.

Y, no solo las entidades que integren este enfoque cumplirán mejor con las expectativas regulatorias, construirán la confianza del cliente y desarrollarán un modelo de negocio más flexible, sino que también crearán confianza y solidez para su modelo de negocio dentro de un entorno acelerado en el que el crimen continúa desbordándose en un mundo más incierto que nunca.

José Frías Hernando
Responsable Blanqueo de Capitales

Evolución tecnológica de las herramientas de prevención de fraude

Artículo por Francisco José García Spina

El fraude financiero ha entrado en una etapa radicalmente distinta. Las mulas de dinero y las estafas avanzadas han dejado de ser incidentes puntuales para convertirse en amenazas coordinadas capaces de impactar simultáneamente a múltiples entidades. La combinación de pagos inmediatos, ecosistemas *fintech* abiertos e identidades digitales vulnerables ha ampliado el perímetro de riesgo y ha obligado al sector financiero a evolucionar su *stack* tecnológico antifraude con más rapidez que nunca.

En este contexto, el reto ya no consiste en identificar una transacción anómala, sino en detener redes enteras, dinámicas y distribuidas, que se adaptan continuamente para evadir controles.

Durante años, las herramientas de prevención se apoyaron en reglas estáticas y en controles diseñados para un ecosistema digital más estable. Ese enfoque ha quedado superado. El fraude actual se caracteriza por ingeniería social sofisticada, manipulación directa del usuario, suplantación de identidad, uso de identidades sintéticas y redes de mulas que ejecutan patrones de colocación, estratificación y dispersión a gran velocidad. Para responder de forma efectiva, las herramientas modernas deben ir más allá del análisis transaccional y comprender qué hace un cliente, cómo lo hace, desde qué dispositivo, bajo qué señales digitales y dentro de qué red de relaciones.

Esta transformación está dando lugar a una nueva generación de plataformas que incorporan inteligencia artificial avanzada, analítica de grafos, biometría comportamental, orquestación inteligente y arquitecturas capaces de anticipar comportamientos sospechosos en tiempo real.

En este contexto, la analítica avanzada se consolida como el núcleo del modelo antifraude moderno. La analítica descriptiva permite comprender la dimensión real del fenómeno de las mulas y priorizar esfuerzos. Los modelos predictivos y de *machine learning* anticipan el riesgo mediante la identificación de comportamientos anómalos y patrones de red. La analítica prescriptiva traduce ese riesgo en decisiones accionables, equilibrando impacto económico, experiencia de cliente y cumplimiento regulatorio.

La inteligencia artificial aporta, además, aprendizaje continuo y escalabilidad, permitiendo sostener la eficacia antifraude frente a tácticas criminales en constante evolución.

A este enfoque se suma la IA generativa, que actúa como un acelerador operativo: analiza información no estructurada, asiste a los analistas en la investigación de casos complejos y mejora la explicabilidad de las decisiones. No sustituye al criterio humano, sino que amplifica su capacidad y eficiencia.

Comprender el ciclo de la mula: el punto de partida del nuevo enfoque

El ciclo de las mulas, colocación y estratificación sigue siendo válido, pero hoy ocurre con tal velocidad que desborda los modelos tradicionales. La evolución natural ha sido pasar de un monitoreo AML reactivo a uno proactivo y tecnificado, que integra:

- Controles avanzados en el *on-boarding* digital y evaluación temprana de riesgo.
- Alertas inteligentes generadas por modelos de IA.
- Identificación de relaciones mediante grafos.
- Análisis contextual basado en canal, dispositivo y velocidad.

Este modelo relacional permite detectar no solo al usuario sospechoso, sino al *cluster* completo al que pertenece.

IA agéntica: el nuevo músculo operativo antifraude

Una de las innovaciones más relevantes es la aparición de agentes de IA especializados, que automatizan tareas críticas del ciclo de fraude y toman decisiones en milisegundos:

- **Agente de *on-boarding* Seguro:** identifica cuentas sintéticas, dispositivos repetidos y señales de “fábricas de cuentas”.
- **Agente de Activación y Dispersión:** monitoriza transacciones de paso rápido (*pass through*) y recomienda retenciones preventivas.
- **Agente de Orquestación:** combina reglas, modelos y apetito de riesgo para decidir si permitir, escalar o bloquear una operación.

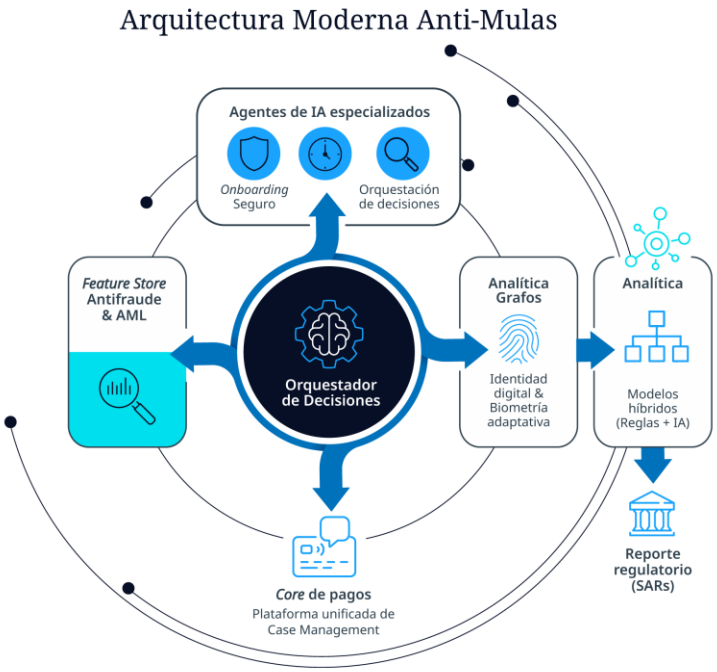
Estos agentes permiten operar al ritmo del fraude moderno, donde la velocidad es clave.

Arquitecturas modernas: de lo transaccional a lo relacional

Las herramientas actuales ya no funcionan como motores independientes, sino como ecosistemas antifraude integrados que combinan analítica de grafos para detectar *clusters* de riesgo.

- Analítica de grafos para detectar clústeres de riesgo.
- Modelos híbridos (reglas + IA) para reducir falsos positivos.
- Señales digitales avanzadas *(Behavioural Biometrics*, *IP Intelligence*, detección de RAT (*Remote Access Trojan*)).
- Trazabilidad completa mediante capacidades de *logging* y *blockchain* en ciertos casos.

El resultado es una detección más precisa y contextual, capaz de anticipar patrones de manipulación humana o automatizada.



El futuro: colaboración interbancaria y *federated learning*

El siguiente salto evolutivo consiste en la detección colaborativa entre entidades. A través de *federated learning*, los bancos pueden compartir inteligencia sin exponer datos sensibles. Esto permitirá:

- Detectar mulas que operan en múltiples entidades.
- Identificar dispositivos o identidades repetidas en el ecosistema.
- Anticipar campañas criminales antes de que se propaguen.

Conclusión

El sector financiero vive una transformación estructural en su lucha contra el fraude. Las reglas estáticas ya no son suficientes. Las herramientas modernas incorporan IA, grafos, señales digitales y arquitecturas inteligentes que permiten desmantelar redes completas y anticiparse a los ataques.

La misión ya no es solo detener operaciones fraudulentas: es comprender la red, anticipar el riesgo y actuar antes de que el fraude se materialice

Francisco José García Spina
Responsable soluciones FinCrime

Impacto operacional de las mulas

Artículo por Carlos Campos Hervas

Desde el punto de vista de operaciones, una vez que han fallado los mecanismos de prevención en evitar su entrada, la gestión de las mulas persigue la detección de estas lo más temprano posible, para evitar su operativa, identificar otras posibles mulas y, posteriormente, el cese de relaciones (cancelación de cuentas y baja de cliente…etc). Es posible detectar una mula en tres momentos de su "ciclo de vida": *On-boarding* ,"Latencia" y Transaccionalidad.

On-boarding

Desde el punto de vista de operación, el *On-boarding* consiste en la verificación de la identidad y documentación y demás datos del cliente. Salvo en caso muy claros, como el uso de un mismo móvil o dirección por "N" personas, irregularidades en la documentación o alertas en la verificación de la identidad (fotos/vídeos), es realmente complejo identificar una mula en la entrada para lo que se están desarrollando modelos específicos.

Este último punto, la verificación de la identidad, es donde las herramientas están avanzando más, permitiendo identificar con mayor precisión caras "n-plicadas" o caras ya existentes en la base de datos de personas ilegitimas. Por otra parte, las herramientas de IA permiten a la delincuencia generar imágenes con mucha mayor exactitud y rapidez. Se dan casos de personas con cientos de intentos de *on-boarding* con caras o identificaciones distintas, por lo que los avances en detección se van compensando con los avances en generación de identidades falsas.

Los procesos de control dentro del marco de AML (*Anti-Money Laundering*) como es el KYC tampoco aportan mucha más información que permita esta detección, ya que muchas personas se dan de alta como estudiantes, amas de casa, etc., que son perfiles con requerimientos de documentación muy escasos.

Latencia

Es durante la vida de las mulas, analizando el movimiento de sus cuentas cuando es posible empezar a detectarlas con mayor fiabilidad.
Se están desarrollando modelos de ML (*Money Laundering*) proactivos que permiten asignar un *rating* a cada persona o cuenta, indicando así la posibilidad de que sea fraudulenta.

Esto modelos se basan en la tipología, cantidad de productos, servicios, operativa, etc., que una cuenta tiene asociadas.

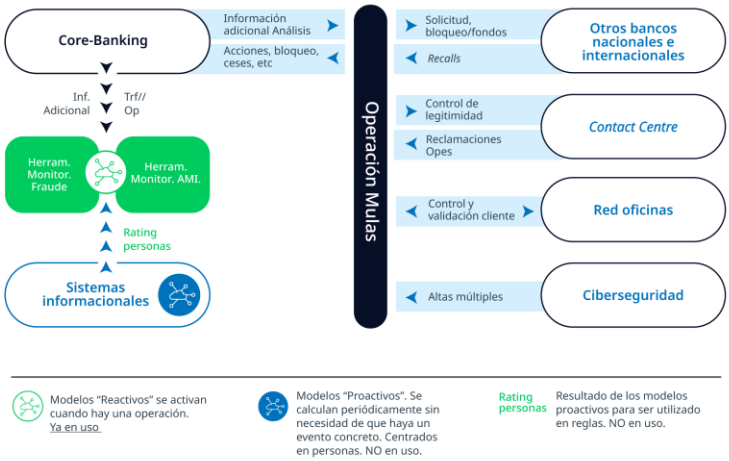
A modo de ejemplo, una cuenta que tenga recibos domiciliados recibe una nómina y en la que se cargan los recibos de un préstamo tiene muchas menos posibilidades de ser una cuenta mula que una de reciente creación, *on-boarding* digital, tipo de cliente estudiante, sin productos ni servicios asociadas, con un saldo medio bajo y operativa frecuente de entrada y salida.

La importancia y efectividad de estos modelos se evidencia cuando son integrados con las herramientas de monitorización de transacciones, ya sean de entrada (AML) o salida (fraude).

Transaccionalidad

La monitorización de transacciones es la pieza clave en la cadena de operación en la detección de las mulas. Básicamente consiste en:

- Análisis de las alertas que son generadas por las herramientas de monitorización
- Toma de acciones en función del resultado del análisis, acciones que pueden generar mucha fricción con clientes como: bloqueo de cuentas, usuario, tarjetas, etc.
- Verificación de legitimidad: se solicita información y documentación adicional para validar si es realmente una mula o se trata de falso positivo
- Cese de relación en caso de confirmación o deshacer las acciones tomadas en caso de falso positivo



Las herramientas de monitorización de transacciones, ya sean de fraude o de AML, están basadas en modelos de ML, pero son reactivos. Al analizar cada operación junto con más información relacionada con cliente, dispositivos, firmas… en el momento que esta se produce.

Al ser UNA monitorización en tiempo real, a pesar de que ha crecido mucho, el volumen de información que pueden procesar sigue teniendo limitaciones, por lo que integrar el resultado de los modelos proactivos en estas herramientas está siendo un gran avance.

Según el origen y destino de los fondos se trata a las mulas de forma distinta.

1. Son operaciones en las que la cuenta de la víctima y la cuenta de la mula están en la misma entidad, en la que estamos "monitorizando". En este caso, la mula se intenta detectar con las herramientas de monitorización de fraude (operaciones de salida de la cuenta origen) que se basan en validar la "habitualidad" en el tipo de operación que está haciendo la "victima". En este tipo de operaciones, la integración de los modelos proactivos con las herramientas de monitorización (fraude) es muy importante, pues las reglas son enriquecidas con una información que las hace más fiables y reduce el falso positivo.

2. Una cuenta ("mula") del banco que estamos monitorizando recibe fondos de otro banco externo, ya sea nacional o internacional. Las herramientas de fraude se basan en analizar operaciones de salida. En este caso, al ser de entrada, deben ser tratadas por las herramientas de AML. Como en el caso anterior, la integración de los modelos proactivos con las herramientas de monitorización (AML) es muy importante.

3. La cuenta de la víctima está en un banco que estamos monitorizando, pero los fondos se envían a otro banco, ya sea nacional o extranjero. Se trata de una operación de salida de fondos, pero no tenemos ninguna información sobre la cuenta destino, al tratarse de una cuenta que está en otra entidad.

Se están desarrollando proyectos para tener información compartida de cuentas fraudulentas, pero aún no están 100% operativos.

Este paso facilita en gran medida la labor que hoy en día hace un analista de alertas.

Impacto de los sistemas de agentes en las operaciones

Mas allá de las mejoras basadas en ML para optimizar la detección, los sistemas de agentes van a ser una pieza clave en la eficiencia de las operaciones.

Un ejemplo es cuando, dentro del análisis de una alerta, se pueden tener agentes que pre-analicen: datos del cliente, datos de las transacciones, datos de la cuenta, datos de los servicios/productos y un agente "orquestador" que en base al resultado de los agentes previos realice pre-análisis facilitando en gran medida la labor que hoy en día hace un analista de alertas.

Carlos Campos Hervas
Responsable operaciones FinCrime

Qué nos espera: ¿mulas cuánticas?

Tendencias por María Angeles Gutiérrez Puente

El fenómeno de las mulas de dinero es uno de los pilares operativos del fraude bancario contemporáneo. Estas personas, conscientes o no, sirven como intermediarios para mover fondos ilícitos y dificultar su rastreo. Sin embargo, la irrupción de la computación cuántica y la criptografía cuántica pueden transformar radicalmente tanto la forma de operar de los ciberdelincuentes como las capacidades de defensa de bancos, reguladores y cuerpos policiales.

El riesgo cuántico: un nuevo ecosistema para el fraude

La principal amenaza de la computación cuántica para el sector financiero es su capacidad teórica para romper los esquemas criptográficos clásicos en los que se basan las transacciones bancarias, la autenticación digital y los canales seguros.

Algoritmos como RSA o ECC podrían quedar obsoletos cuando existan ordenadores cuánticos lo suficientemente potentes.

¿Cómo afecta esto a las mulas? De dos formas principalmente:

1. **Fraudes más rápidos y difíciles de rastrear.** Si un atacante logra romper claves o suplantar identidades digitales de forma masiva, podrá generar transacciones fraudulentas que requerirán mulas humanas o digitales para mover el dinero antes de que se detecte el ataque.
2. **Desaparición paulatina de la mula humana**. El fraude evolucionaría hacia esquemas completamente automatizados, donde *bots* y carteras digitales cifradas con técnicas post-cuánticas se encarguen del tránsito de fondos. La "mula cuántica" sería un *software* distribuido y anónimo, muy difícil de bloquear.

Criptografía cuántica y post-cuántica: contramedidas que favorecen a los defensores

Por otro lado, las comunicaciones cuánticas, especialmente la distribución cuántica de claves (QKD), ofrece una capacidad inédita: detectar cualquier intento de interceptación gracias al principio de no clonación cuántica.

Si los bancos adoptan QKD entre centros críticos, las comunicaciones interbancarias se volverán prácticamente imposibles de espiar incluso para un adversario con un ordenador cuántico.

Además, la criptografía post-cuántica (PQC), ya estandarizada por NIST, permitirá a reguladores y entidades migrar a sistemas resistentes a ataques cuánticos antes de que estos existan.

Esto significa:

- Menos posibilidad de ataques que generen transferencias fraudulentas, reduciendo el volumen de dinero ilícito que necesitaría ser blanqueado.
- Mejor trazabilidad: muchos algoritmos post-cuánticos permiten autenticación fuerte sin comprometer metadatos necesarios para investigaciones.
- Mayor protección de identidades y pruebas digitales dentro de investigaciones policiales.

Los beneficios para la investigación criminal

La computación cuántica también tiene potencial para mejorar las capacidades forenses, por ejemplo:

- Analizar grandes grafos de transacciones para detectar patrones de mulas con mayor profundidad y velocidad.
- Optimizar la correlación entre cuentas, dispositivos y comportamientos.
- Acelerar el análisis de *blockchain* en investigaciones de "criptofraude".

No se trata solo de rastrear mejor, sino de anticipar comportamientos gracias a modelos cuánticos aplicados a series temporales y flujos financieros.

Los reguladores ante el desafío cuántico

Los organismos reguladores tendrán que:

- Exigir la migración obligatoria a criptografía post-cuántica.
- Establecer normas claras para el uso de QKD en infraestructuras críticas.
- Preparar marcos legales para escenarios en los que las mulas sean *software* autónomo.

Maria Angeles Gutiérrez Puente
Responsable Ciberseguridad / Cuántica FinCrime

Vulnerabilidades

Vulnerabilidad crítica en SolarWinds Web Help Desk

Fecha: 29 de enero de 2026
CVE: CVE-2025-40551

CVSS: 9.8

CRÍTICA

Descripción

Se ha identificado una vulnerabilidad crítica, catalogada como **CVE-2025-40551**, que afecta a SolarWinds Web Help Desk. El fallo está relacionado con un problema de deserialización de datos no confiables.

La deserialización es el proceso mediante el cual una aplicación convierte un flujo de datos, como una cadena de texto o una secuencia de *bytes*, en objetos utilizables dentro del entorno operativo.

En este caso, la vulnerabilidad podría permitir la ejecución remota de código (RCE), lo posibilita que un atacante no autenticado ejecute comandos arbitrarios en el servidor afectado, comprometiendo la seguridad del sistema.

Solución

Se recomienda:

- Limitar la exposición a Internet y revisar los *logs*.
- Actualizar los servidores vulnerables a Web Help Desk a la versión 2026.01.

Productos afectados

SolarWinds Web Help Desk en las versiones 12.8.8 HF1 y todas las anteriores.

Referencias

- thehackernews.com
- incibe.es
- solarwinds.com

TLP:WHITE

Vulnerabilidades

Vulnerabilidad crítica en Ivanti EPMM

Fecha: 30 de enero de 2026
CVE: CVE-2026-1281 y una más

CVSS: 9.8

CRÍTICA

Descripción

Se han identificado vulnerabilidades críticas de inyección de código en Ivanti Endpoint Manager Mobile (EPMM).

Estas vulnerabilidades (**CVE-2026-1281** y **CVE-2026-1340**) permiten a un atacante ejecutar código remoto sin necesidad de autenticación, afectando a componentes internos de EPMM. Ivanti ha confirmado que, al menos una de ellas, ha sido explotada activamente en un número limitado de casos.

La explotación exitosa podría permitir el control total del sistema EPMM, comprometiendo la gestión de dispositivos móviles y el acceso a recursos corporativos.

Solución

Se recomienda:

- Aplicar inmediatamente el *hotfix* proporcionado por Ivanti: RPM 12.x.0 or 12.x.1 (teniendo en cuenta que el *hotfix* no persiste tras una actualización de versión y deberá replicarse).
- Actualizar a la versión 12.8.0.0, que incluirá la corrección permanente (prevista para Q1 2026).

Productos afectados

Ivanti Endpoint Manager Mobile (EPMM) en las siguientes versiones:

- 12.5.1.0 y anteriores
- 12.6.1.0 y anteriores
- 12.7.0.0 y anteriores

Referencias

- nvd.nist.gov
- hub.ivanti.com

Microsoft corrige vulnerabilidad *Zero-Day* crítica en Microsoft Office

Fecha: 26 de enero de 2026
CVE: CVE-2026-21509

Crítica

Descripción

La vulnerabilidad **CVE-2026-21509,** consiste en un *bypass* de mecanismos de seguridad en Microsoft Office. La misma permite a un atacante evadir las protecciones mediante documentos especialmente diseñados.

Su explotación requiere que la víctima abra el archivo malicioso, lo que puede derivar en la ejecución de acciones no autorizadas que comprometan la seguridad del equipo.

Se confirmó que la vulnerabilidad estaba siendo explotada activamente por atacantes. Ante esta situación, Microsoft publicó un parche de emergencia para corregirla de forma inmediata.

Productos afectados

Los productos afectados por esta vulnerabilidad incluyen:

- Microsoft Office 2016
- Microsoft Office 2019
- Office LTSC 2021/2024
- Microsoft 365 Apps

Solución

Se recomienda:

- Aplicar inmediatamente las actualizaciones de seguridad publicadas por Microsoft mediante Windows Update o Microsoft Update.
- r

Referencias

- cyber.gov.rw
- msrc.microsoft.com

TLP:WHITE

Fortinet corrige una vulnerabilidad crítica de omisión de autenticación

Fecha: 28 de enero de 2026
CVE: CVE-2026-24858

Crítica

Descripción

La vulnerabilidad crítica **CVE-2026-24858** corresponde a una omisión de autenticación en FortiOS, el sistema operativo basado en el *kernel* de Linux que utilizan los dispositivos de Fortinet.

El fallo podría permitir que un atacante con una cuenta de FortiCloud y un dispositivo registrado accediera a otros equipos y cuentas sin autenticación. Esta capacidad se habría utilizado para crear cuentas locales con privilegios de administrador, mantener persistencia, modificar configuraciones, habilitar accesos VPN y exfiltrar la configuración del *firewall*.

La vulnerabilidad afectaba a varios productos del ecosistema Fortinet, entre ellos FortiManager y FortiProxy.

Productos afectados

Los productos afectados por esta vulnerabilidad incluyen:

- Los servicios de FortiManager y FortiAnalyzer en las versiones anteriores a la 7.6.0 (incluida).
- FortiProxy versiones anteriores a la 7.6.4 (incluida).
- FortiWeb desde la versión 7.4.0 hasta la 8.0.3

Solución

Se recomienda:

- Actualizar a las últimas versiones del *software*.
- Resetear las credenciales posiblemente afectadas.

Referencias

- thehackernews.com
- incibe.es

Eventos

RootedCON 2026
5 - 7 de marzo

Madrid se prepara para acoger una nueva edición de RootedCON 2026, uno de los congresos de ciberseguridad más relevantes del panorama nacional e internacional. El evento, que volverá a reunir a expertos técnicos, investigadores, responsables de seguridad, fuerzas y cuerpos de seguridad del Estado y empresas tecnológicas, se consolida como un espacio estratégico para el intercambio de conocimiento y la actualización frente a las amenazas emergentes.

Enlace

Ohio Information Security Conference
11 de marzo

La Ohio Information Security Conference (OISC) 2026 se perfila como una de las citas más importantes en el calendario de ciberseguridad para profesionales técnicos y gestores de riesgos. Organizada por Technology First, esta conferencia anual reunirá el 11 de marzo de 2026 en el Sinclair Conference Center de Dayton (Ohio, EE. UU.) a expertos, analistas, CISOs y equipos de seguridad para analizar las últimas amenazas, estrategias de respuesta en tiempo real y soluciones innovadoras ante riesgos emergentes como los impulsados por IA, además de facilitar networking, talleres y demos de tecnologías de defensa.

Enlace

RSAC Conference
23 - 26 de marzo

La RSAC Conference 2026, considerada una de las citas más influyentes del calendario global de ciberseguridad, volverá a reunir a miles de profesionales del sector del 23 al 26 de marzo de 2026 en el Moscone Center de San Francisco (EE. UU.). El evento —donde "el mundo habla de seguridad"— sirve como plataforma para explorar las tendencias que están dando forma al futuro digital, con ponencias, sesiones técnicas y exposiciones sobre temas clave como inteligencia artificial, gestión de riesgos, identidad y defensa ante amenazas emergentes, así como oportunidades de *networking* entre investigadores, CISOs y proveedores de soluciones. La conferencia se ha consolidado como un espacio de referencia para compartir estrategias de defensa, analizar incidentes recientes y fomentar la innovación en seguridad informática.

Enlace

5º Congreso de Ciberseguridad de Andalucia
24 - 25 de marzo

Málaga se prepara para acoger los días 24 y 25 de marzo de 2026 el 5º Congreso de Ciberseguridad de Andalucía, un foro anual que se ha consolidado como punto de encuentro clave para el ecosistema de seguridad digital en el sur de España. Organizado por la Agencia Digital de Andalucía en colaboración con el Ayuntamiento de Málaga, el evento reunirá a especialistas, responsables institucionales, empresas tecnológicas, *start-ups* y *pymes* para debatir sobre protección de datos, ciberresiliencia, seguridad en entornos *cloud*, inteligencia artificial aplicada a la defensa digital y la creciente necesidad de talento especializado en ciberseguridad.

Enlace

Recursos

➢ *Checklist* de mejores prácticas

Lista actual de acciones ciberseguridad con enfoque operacional: controles de identidad, actualizaciones críticas, *backups* verificados, *vendor controls*... perfecta como *checklist* para inspecciones rápidas o auditorías internas.

Enlace

➢ Global Cybersecurity Outlook 2025 – Foro Económico Mundial (WEF)

Un informe estratégico y global que examina cómo la ciberseguridad está evolucionando frente a tecnologías emergentes, tensiones geopolíticas y retos de resiliencia. Proporciona datos clave sobre riesgos como la dependencia de las cadenas de suministro, la sofisticación de los ataques y disparidades en capacidades entre organizaciones, con recomendaciones para líderes que deben navegar esta complejidad creciente.

Enlace

➢ GCA Cybersecurity Toolkit (Global Cyber Alliance)

Un *kit* de herramientas y guías prácticas para evaluar la postura de seguridad, reforzar controles comunes y acceder a soluciones gratuitas con enfoque claro en defensas básicas recomendadas internacionalmente.

Enlace

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com