Edición 360 ADAPTIVE AUTHENTICATION

FRAUD BEAT: PERSPECTIVAS ESTRATÉGICAS

UN ENFOQUE EN LA INDUSTRIA FINANCIERA

appgate

TABLA DE CONTENIDOS

Un vistazo rápido a los titulares globales de hoy y a los informes de investigación relacionados con la industria revela las crecientes presiones y los cambios significativos que enfrentan las instituciones financieras. Estos desafíos están impulsados por varios factores clave:

1 / ***Perspectivas macroeconómicas inciertas:*** La mayor volatilidad económica mundial ha aumentado, con expectativas de crecimiento e inflación variables en las distintas regiones, lo que crea un entorno económico incierto propicio para el fraude y los ciberataques, ya que los actores malintencionados buscan explotar las disparidades regulatorias y la inestabilidad económica.

2 / ***Regulación y supervisión gubernamental más estrictas:*** Las nuevas regulaciones, como el Endgame de Basilea III, imponen requisitos de capital más estrictos a los bancos grandes y medianos, incluidos estándares de ciberseguridad más estrictos para proteger la integridad y la seguridad de las operaciones financieras.

3 / ***Disrupción tecnológica:*** La rápida adopción de la inteligencia artificial (IA) y el aprendizaje automático (ML) está transformando la industria, particularmente en la detección y prevención de fraudes. Estas tecnologías avanzadas mejoran la seguridad de las transacciones digitales al identificar y mitigar las amenazas en tiempo real. Sin embargo, la creciente sofisticación de las ciberamenazas que utilizan la misma tecnología exige una innovación continua en soluciones avanzadas contra el fraude para mantenerse por delante de los actores maliciosos.

4 / ***Riesgo sistémico:*** El aumento de las tensiones geopolíticas y las restricciones comerciales aumentan la volatilidad y el riesgo sistémico, con ciberataques patrocinados por Estados y actores maliciosos que amenazan la estabilidad de las instituciones financieras mundiales. Las defensas cibernéticas sólidas son fundamentales para mitigar estos riesgos.

5 / **Mayor conectividad y movilidad:** La innovación tecnológica y las interdependencias económicas han aumentado la comunicación y la movilidad, así como la velocidad de la innovación en la industria financiera. Sin embargo, esta mayor conectividad también facilita la rápida difusión de información y desinformación, que puede desestabilizar a los bancos.

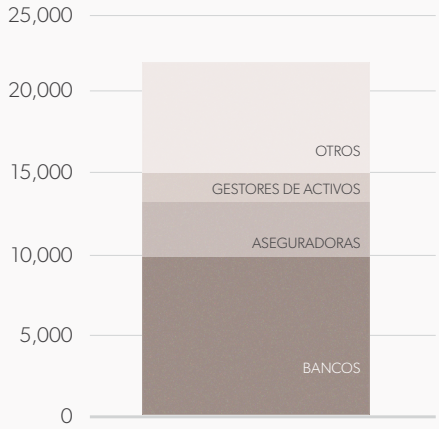
En 2024, el efecto de goteo de estas presiones es evidente. Uno de los bancos más grandes del mundo, JPMorgan Chase, informó recientemente que lucha contra aproximadamente 45 mil millones de intentos de piratería por día. E incidentes como la muy publicitada violación de datos de Bank of America en febrero de 2024 causada por un proveedor externo comprometido, subrayan cuán interconectados están los sistemas de TI en toda la industria financiera y la necesidad de defensas integrales y de múltiples capas.

Este informe de Fraud Beat se centra en el crecimiento explosivo de los canales transaccionales financieros digitales en pagos, cobros, inversiones y ahorros. Ofrece inteligencia rica en datos y orientación práctica que las instituciones financieras pueden utilizar para potenciar su capacidad de detectar y detener transacciones fraudulentas antes de incurrir en pérdidas monetarias y daños irreparables a la reputación.

TENDENCIAS GLOBALES DE FRAUDE *DE INSTITUCIONES FINANCIERAS*

Las instituciones financieras son el objetivo favorito de los actores de amenazas que buscan robar fondos o datos para obtener ganancias monetarias, o de los estados nacionales centrados en objetivos más nefastos, como perturbar la estabilidad mundial. Según el Informe sobre la **Estabilidad Financiera Mundial 2024 del Fondo Monetario Internacional**, casi el 20% de los incidentes cibernéticos notificados entre 2004 y 2023 afectaron a este sector, siendo los bancos el principal objetivo. El GFSR estima pérdidas directas en casi 12.000 millones de dólares durante este tiempo, de los cuales 2.500 millones de dólares se registraron a partir de 2020, lo que indica una escalada en las violaciones exitosas de las instituciones financieras.

Incidentes cibernéticos en el sector financiero
(número, 2004-23)



Pérdidas en el sector financiero
(mil millones de USD, 2004-23)

Como se destaca en el informe del GFSR, las pérdidas financieras directas resultantes del fraude son sustanciales y preocupantes. Sin embargo, las pérdidas indirectas resultantes de actividades fraudulentas, como el daño a la reputación o la necesidad de actualizaciones de seguridad, pueden superar con creces este impacto financiero directo. La protección de estas instituciones es primordial, ya que los incidentes en el sector financiero pueden tener consecuencias de gran alcance. Los ciberataques pueden erosionar la confianza en el sistema financiero, interrumpir servicios críticos y desencadenar un efecto dominó en otras instituciones, amenazando en última instancia la estabilidad financiera y económica mundial.

EN CIFRAS: EL PODER DE LA PROTECCIÓN CONTRA ANOMALÍAS EN LAS TRANSACCIONES

Impulsada por la IA, la solución de Detección de Anomalías en las Transacciones (DTA por sus siglas en inglés), una poderosa herramienta de la suite de protección contra el fraude multicapa 360 Adaptive Authentication de Appgate, analiza miles de millones de transacciones en todo el mundo para identificar y detener los ataques maliciosos. En 2023, DTA analizó más de 2 mil millones de transacciones solo en América del Norte y LATAM, frustrando un estimado de $73.5 millones de dólares en pérdidas monetarias debido al fraude. Esto representa un aumento del 37% en las transacciones analizadas y un aumento del 177% en la prevención de pérdidas por fraude en comparación con 2022.

América del Norte		**Latinoamérica**	
TOTAL DE TRANSACCIONES ANALIZADAS	**612M**	TOTAL DE TRANSACCIONES ANALIZADAS	**1.450M**
PROMEDIO DE TRANSACCIONES DIARIAS	**1.7M**	PROMEDIO DE TRANSACCIONES DIARIAS	**4.0M**
PROMEDIO DE ALERTAS DIARIAS	**32**	PROMEDIO DE ALERTAS DIARIAS	**45**
PÉRDIDAS ANUALES EVITADAS	**USD $33M**	PÉRDIDAS ANUALES EVITADAS	**USD $40M**

En América del Norte, se analizaron automáticamente 612 millones de transacciones, lo que equivale a un promedio diario de 1,7 millones, y se bloquearon las transacciones sospechosas, lo que equivale a una prevención de pérdidas de aproximadamente $ 33 millones de dólares. En América Latina, se analizaron 1.45 mil millones de transacciones, lo que equivale a un promedio diario de 4 millones, lo que equivale a una prevención de pérdidas de aproximadamente $ 40 millones de dólares.

La diferencia de volumen desproporcionada refuerza lo que sabemos que es cierto cuando se trata de tendencias de transacciones digitales en LATAM:

Esfuerzos de inclusión financiera: Los gobiernos regionales y las instituciones financieras han estado trabajando activamente para aumentar la inclusión financiera. Los servicios financieros digitales, incluida la banca móvil y las billeteras digitales, permiten a la población no bancarizada acceder a servicios financieros y participar en la economía digital.

Soluciones fintech innovadoras: LATAM es una incubadora de fintech con la introducción de nuevos productos y servicios financieros que se adaptan a las necesidades de la región. Estos incluyen sistemas de pago móvil, préstamos entre pares y monedas digitales.

Demografía joven: La población de LATAM es relativamente joven y conocedora de la tecnología. Los consumidores más jóvenes están más inclinados a adoptar métodos de pago digitales y compras en línea, lo que contribuye al aumento de las transacciones digitales.

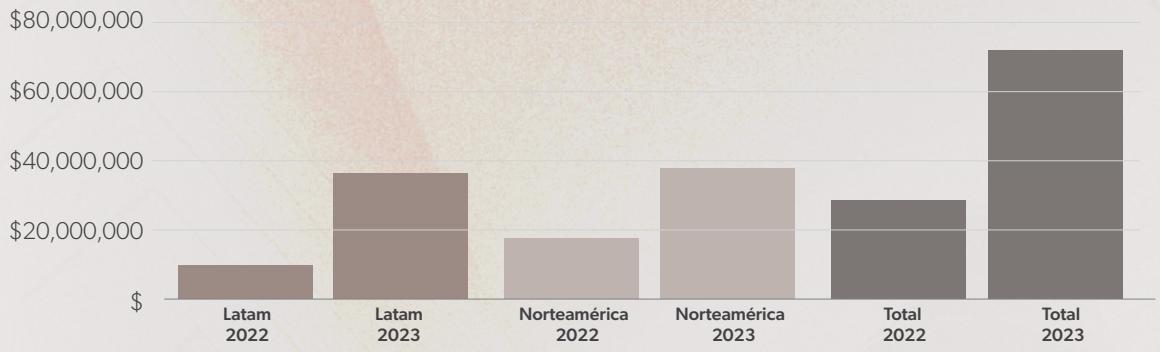
Crecimiento del comercio electrónico: El auge de las plataformas de comercio electrónico en la región impulsa las transacciones digitales.

En 2023, las capacidades de automatización impulsadas por IA de DTA también redujeron significativamente el número de alertas diarias que deben gestionar los equipos internos de prevención del fraude. El promedio de alertas diarias fue de 32 y 45 para Norteamérica y LATAM, respectivamente. Esta ventaja significa que las instituciones financieras pueden reducir los costos operativos hasta en un 80%, optimizar sus recursos y mejorar la eficiencia administrativa. Esto es especialmente cierto si se tiene en cuenta que las estimaciones del sector sugieren que los equipos de servicios financieros pueden recibir entre 100 y 3.000 alertas al día, y en algunos casos hay entre 10.000 y 15.000 alertas diarias.

ANÁLISIS DE DATOS
COMPARATIVOS DE DTA

Al comparar 2023 con 2022, tanto América del Norte como América Latina experimentaron un aumento sustancial en las transacciones analizadas, lo que refleja una creciente dependencia de las transacciones digitales y los importantes avances de DTA en la detección y bloqueo automático de anomalías fraudulentas en todo el mundo en 2023. Impulsada por IA y ML, la solución DTA de Appgate ha mejorado significativamente la detección y prevención de fraudes, lo que ha llevado a un aumento notable en el volumen de intentos de fraude bloqueados para los clientes. Profundicemos en los datos:

Pérdidas financieras prevenidas



El tamaño de la muestra reportada es un porcentaje consistente de clientes de Appgate, que se mantuvo en el mismo nivel de 2022 a 2023 con el fin de ilustrar una línea de base para comparar la evolución del panorama de amenazas y las tendencias transaccionales. Los datos presentados subrayan el valor de la solución DTA de Appgate, que proporciona una sólida detección y prevención del fraude que mejora la seguridad y la eficiencia operativa.

***DTA de Appgate** analizó más de 2.000 millones de transacciones y evitó 73,5 millones de dólares en pérdidas fraudulentas*

Valores representativos de monedas locales convertidos a dólares estadounidenses según los tipos de cambio al momento de la generación del informe.

EL ENFOQUE COMPROBADO DE APPGATE PARA LA PREVENCIÓN DEL FRAUDE

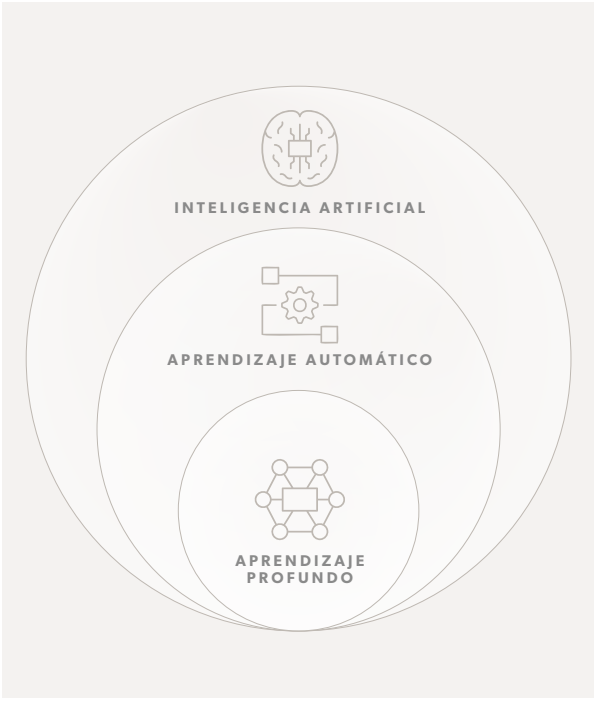
DTA de Appgate es una solución de prevención de fraude que ayuda a las organizaciones a detectar actividades fraudulentas en sus transacciones en tiempo real. Aprovecha los evaluadores interconectados derivados de IA, incluido el ML y su subconjunto aprendizaje profundo (DL). Como **IBM** lo define, el aprendizaje profundo" es un subconjunto de aprendizaje automático que es una red neuronal con tres o más capas. Estas redes neuronales intentan emular el comportamiento del cerebro humano, y esto le permite "aprender" de cantidades sustanciales de datos. Aunque una red neuronal de una sola capa ya puede hacer predicciones aproximadas, las capas ocultas adicionales ayudan a optimizar y refinar la precisión".

El aprendizaje profundo es una fuerza impulsora en el avance de la IA, ya que permite la automatización de tareas analíticas de gran volumen, lo que conduce a una toma de decisiones más precisa.

A continuación, se presentan tecnologías de análisis de datos adicionales, más allá de las mencionadas anteriormente, que permiten a Appgate generar alertas de fraude precisas mediante la identificación de anomalías y patrones en las transacciones de los clientes en tiempo real.

ADICIONALES INCLUYEN:

- **Reglas institucionales:** Cree restricciones basadas en parámetros personalizados en tiempo real.
- **Analizadores de actividades sospechosas:** Busque fraude en un conjunto de patrones de transacción, atacando la ruta crítica del fraude tan pronto como se detecte.
- **Analizadores en tiempo real:** Aproveche la detección heurística y de anomalías para permitir el monitoreo en tiempo real de las transacciones, lo que reduce la fricción con los clientes.
- **Evaluaciones compuestas:** Combinar diferentes evaluadores.



LOS EVALUADORES

Estas mejoras subrayan el valor de la solución DTA de Appgate, reforzando su capacidad para ofrecer una sólida detección y prevención de fraudes que contribuye directamente a la seguridad financiera y la eficiencia operativa de nuestros clientes.

CUATRO ETAPAS FUNDAMENTALES DE LA PREVENCIÓN DEL FRAUDE

Lograr una sólida prevención del fraude está al alcance de la mano. Si bien la implementación de una solución integral de prevención de fraude como parte de una iniciativa de transformación digital, incluida la integración de varios productos de software y áreas organizativas para mitigar el fraude y fortalecer la seguridad financiera, puede ser compleja, no tiene por qué ser abrumadora. El experimentado equipo de Appgate puede guiarlo a través de las mejores prácticas, asegurando una implementación fluida y eficiente.

Una solución integral de prevención de fraude es el resultado de un sistema bien coordinado compuesto por procesos, procedimientos, equipos interdisciplinarios y tecnología que trabajan en armonía.

El enfoque de Appgate para una solución exitosa de prevención de fraude se basa en una base de prácticas fundamentales diseñadas para reducir la complejidad. Estas prácticas se dividen en cuatro fases clave:

- ***Fase 1:*** Evaluación de la madurez de la gobernanza del fraude
- ***Fase 2:*** Alineación de expectativas
- ***Fase 3:*** Implementación
- ***Fase 4:*** Operación

Al abordar la prevención del fraude como un proceso holístico y realizar un seguimiento del rendimiento a través de indicadores clave de rendimiento (KPI) definidos, las organizaciones pueden obtener una hoja de ruta clara para la mejora continua y la evolución estratégica. Cada ciclo a través de estas fases debe representar un refinamiento iterativo de la estrategia general de prevención del fraude.

Los servicios profesionales de Appgate siguen estas fases estandarizadas, al tiempo que adaptan la ejecución a los requisitos específicos de cada cliente. Nuestro enfoque colaborativo fomenta una cultura de investigación, pensamiento crítico y una comprensión profunda de los riesgos de fraude. Nos esforzamos por crear valor compartido tanto para Appgate como para nuestros clientes, beneficiando en última instancia a los usuarios finales que confían en nuestras soluciones.

Appgate satisface las necesidades específicas de las instituciones financieras y no financieras:

Entidades financieras: Hemos observado un crecimiento significativo en la adopción de sólidas estrategias de gobernanza y prevención del fraude dentro de las instituciones financieras. Sin embargo, algunas organizaciones pueden priorizar el cumplimiento normativo sobre una estrategia más amplia. Esto a veces puede conducir a conversaciones complejas y plazos de implementación más largos. El enfoque de cuatro fases de Appgate puede ayudar a agilizar este proceso.

Entidades no financieras: Para este grupo en expansión, el DTA de Appgate a menudo requiere una configuración, supervisión y ajuste más extensos a lo largo de las fases. Esto se debe a la amplia gama de escenarios de fraude y a los limitados precedentes regulatorios en comparación con las instituciones financieras. Esta tendencia es evidencia de que el fraude se extiende más allá del sector financiero, y las organizaciones no financieras reconocen cada vez más que sus servicios, reputación y experiencia del cliente son activos valiosos que vale la pena proteger.

PROTECCIÓN CONTRA EL FRAUDE *360 DE APPGATE*

Appgate 360 Fraud Protection, que comprende 360 Brand Guardian y 360 Adaptive Authentication, es una plataforma de seguridad integral y multicapa diseñada para combatir todas las formas de fraude en línea. Protege todas las etapas del ciclo de ataque, desde la planificación inicial hasta el cobro. Aprovechando un motor basado en IA que se adapta al comportamiento del usuario, la solución detecta y mitiga las amenazas en tiempo real, neutralizando los posibles ataques antes de que causen daños irreparables al negocio. Si bien cada capa de la plataforma Appgate 360 Fraud Protection funciona de forma independiente y eficaz, el poder de la plataforma se amplifica cuando las capas se integran como una suite. Esta integración permite compartir sin problemas la inteligencia contra el fraude entre capas, lo que mejora la eficacia general del sistema de protección contra el fraude.

Acerca de **360 Brand Guardian**

360 Brand Guardian de Appgate es una solución integral diseñada para salvaguardar su marca digital. Está diseñado para proporcionar una detección avanzada de suplantación de identidad, lo que permite a las organizaciones identificar y mitigar actividades fraudulentas que introducen un riesgo significativo para la integridad de la marca y la confianza del cliente. 360 Brand Guardian permite a las empresas eliminar de forma proactiva a los impostores y los sitios falsos destinados a robar las credenciales de los clientes:

- **Digital Threat Protection (DTP):** Ofrece un enfoque integral y multicanal para analizar y monitorear continuamente la web, las redes sociales y las fuentes de datos públicos. Permite una protección proactiva contra amenazas externas al detectarlas y eliminarlas, independientemente del tamaño de la población de usuarios. Esta solución reduce significativamente la actividad delictiva y mitiga el riesgo de futuros ataques.

- **Digital Risk Protection (DRP):** Descubre credenciales de empleados comprometidas, tarjetas de crédito robadas y código fuente expuesto en repositorios públicos. La solución identifica los datos robados y expuestos en la Dark Web y la Deep Web, lo que permite una acción rápida para evitar estafas o fugas de datos dentro de los sistemas de la organización.

- **Appgate Email Protection:** Mitiga el riesgo de phishing, malware y amenazas transmitidas por correo electrónico utilizando métodos avanzados de protección de correo electrónico como DMARC, BIMI, SPF y DKIM. La solución detecta y neutraliza eficazmente los correos maliciosos.

Acerca de **360 Adaptive Authentication**

La autenticación adaptativa 360 de Appgate proporciona una autenticación sin fricciones para salvaguardar las operaciones y las experiencias de los clientes sin incomodar a los usuarios finales, todo desde un único punto de control. A través de análisis de comportamiento avanzados y técnicas basadas en riesgos, la solución evalúa continuamente las acciones del usuario, las características del dispositivo y los patrones de sesión para ofrecer una protección dinámica contra el fraude complejo. Sus completos sensores de riesgo garantizan un entorno seguro y de confianza, manteniendo la confianza del usuario y la reputación de la marca. 360 Adaptive Authentication ofrece una protección dinámica, personalizable y basada en el riesgo y el comportamiento que elimina la fricción del usuario y los bloqueos de falsos positivos con:

- **Detect ID (DID):** Proporciona una autenticación adaptativa sólida para proteger las identidades digitales con autenticación multifactor (MFA), evaluación de riesgos en tiempo real e interfaces fáciles de usar. La solución adapta de forma inteligente los métodos de autenticación a medida que surgen nuevos riesgos, lo que garantiza un acceso seguro a través de varios canales.

- **Risk Sensors:** Analice los comportamientos de los usuarios, como la dinámica de las pulsaciones de teclas y los movimientos del ratón, para detectar y prevenir el fraude. La solución garantiza una autenticación sin interrupciones con supervisión continua y aprendizaje adaptativo, integrándose en todas las plataformas para una protección y comodidad constantese.

- **Detect Transaction Anomalies (DTA):** Aprovecha el aprendizaje automatizado, priorizando las alertas de alto riesgo para mejorar la eficiencia. La solución admite la autenticación en tiempo real basada en riesgos y ofrece integración omnicanal para el monitoreo de transacciones e inicios de sesión. El aprendizaje automático (ML) avanzado y un sistema flexible basado en reglas detectan y mitigan dinámicamente las amenazas de fraude conocidas y emergentes.

RECOMENDACIONES
PARA LA INDUSTRIA FINANCIERA

Como reveló el informe Faces of Fraud, una encuesta realizada a más de 200 instituciones financieras destacó su creciente preocupación por el aumento exponencial del fraude y los desafíos de mantener el ritmo. Para adaptarse a estas tendencias cambiantes y mitigar los riesgos de fraude, las instituciones financieras deben:

- **Implementar soluciones avanzadas de ciberseguridad:** Aproveche la IA y la analítica avanzada para detectar y prevenir el fraude en tiempo real, salvaguardando los datos confidenciales de los clientes.
- **Fortalecer la supervisión y el cumplimiento normativo:** Adopte soluciones sólidas de ciberseguridad para garantizar el cumplimiento de las regulaciones y los estándares de seguridad en evolución.
- **Mejorar la resiliencia frente a los ciberataques:** Desarrolle estrategias integrales de gestión de riesgos cibernéticos para abordar de manera proactiva las amenazas emergentes y mantener la continuidad del negocio.

Al integrar estas recomendaciones, las instituciones financieras pueden fortalecer su posición en el mercado y reforzar la confianza de los clientes en un panorama digital cada vez más dinámico. Para profundizar en las amenazas y soluciones al fraude, explore nuestro Informe Anual 2023 Fraud Beat, un análisis exhaustivo de las tendencias del fraude electrónico a lo largo de 2023.

Descubra cómo el **Monitoreo de Transacciones** DetectTA de Appgate puede ayudar a su organización a identificar y mitigar actividades sospechosas con el poder del aprendizaje automático y el análisis avanzado.