MAPA CRÍTICO DE LAS AMENAZAS 2025
Ataques más sofisticados, difíciles de desactivar y con mayor impacto en la confianza del cliente

Evolución del fraude digital

Para decidir, con datos, dónde enfocar recursos y cómo responder primero.

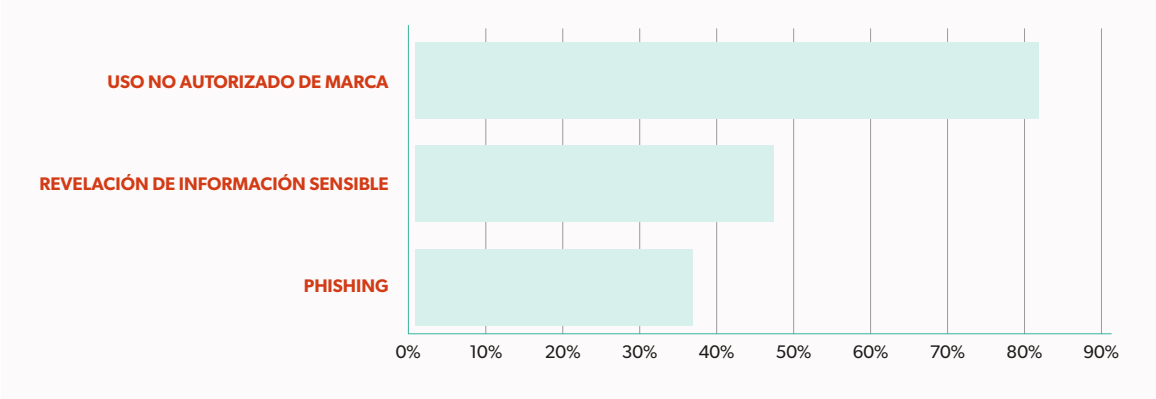
En los últimos seis meses los atacantes pasaron de golpes rápidos a **imitar tu marca en profundidad.** Replican identidad visual y tono, lanzan perfiles y dominios en minutos y explotan brechas operativas para extender la vida de cada incidente. El efecto: más clientes expuestos, mayor carga operativa y una confianza que se erosiona con cada hora de exposición (Phishing Activity Trends Report 2025).

Cómo se está comportando el fraude

Entre H2 2024 y H1 2025, según datos de nuestro Security Operations Center (SOC), **el mayor salto está en los ataques que explotan la identidad de marca.** Además del volumen, aumenta el **tiempo de exposición** de cada ataque y la **diversificación de canales** (social, dominios, apps), lo que dificulta su desactivación rápida.

Los siguientes provienen de nuestro SOC (H1 2025).

- **Uso no autorizado de marca (+81%):** sitios, perfiles y apps falsos que parecen oficiales. El usuario confía, entrega datos y el golpe reputacional llega rápido.
- **Revelación de información sensible (+48%):** Datos expuestos que alimentan fraudes en cadena: ATO, préstamos indebidos, SIM swapping.
- **Phishing (+37%):** La puerta de entrada más barata y escalable, ahora con textos e imágenes generados por IA.



El podio de las amenazas

Datos de nuestro SOC (H1 2025). En la primera mitad de 2025, dos tácticas explican 95 % de los incidentes: uso no autorizado de marca (50 %) y phishing (45 %). La revelación de información sensible (4 %) parece menor, pero suele ser el combustible de ataques posteriores. Concentrar recursos en estas dos tácticas ofrece el mayor retorno de mitigación. Para reforzar: el phishing y la ingeniería social siguen entre los vectores más comunes a nivel global (Verizon DBIR 2025). Fuente

Mapa regional: no todas las regiones son atacadas por igual

La primera mitad de 2025 nos demuestra que ajustar la estrategia por mercado ya no es opcional.

TIPO DE ATAQUE	MEX + CAM* México y Centro América	ANDINA* Colombia, Venezuela, Perú, Ecuador y Bolivia	SUR* Argentina, Chile, Uruguay y Paraguay
PHISHING	42%	70%	15%
REDES SOCIALES FALSAS	39%	28%	84%
USO NO AUTORIZADO DE MARCA	19%	2%	1%

Recomendaciones por región

- **Andina:** Priorizar campañas anti phishing y autenticación adaptativa; incorpora alertas tempranas de dominios sospechosos para cortar el fraude en origen.
- **Sur:** Refuerzar el monitoreo de redes sociales y establece un flujo de takedown express con proveedores para reducir horas de exposición.
- **Mex + CAM:** Combinar monitoreo multicanal (web, social, dominios) con respuestas rápidas y coordinadas entre Riesgo, Marketing y Legal.

El costo real para el negocio

Cada hora que un sitio fraudulento permanece online erosiona la relación con el cliente. **La mediana global de "duración" llegó a 11 días en 2024** (M Trends 2025).

Los gastos posteriores a incidentes también se disparan: el coste medio global de una **filtración de datos es de 4,4 millones de dólares estadounidenses**, lo que supone una disminución del 9 % con respecto al año pasado, gracias a una identificación y contención más rápidas. (IBM Cost of a Data Breach 2025).

Además, la ingeniería social (phishing) se mantiene como el vector más común a nivel global (Verizon DBIR 2025).

Acciones inmediatas y cómo lograrlas con 360 Brand Guardian

Con **360 Brand Guardian** monitoreamos y damos de baja usos indebidos de marca en dominios, redes sociales, app stores y dark web, orquestando todo el ciclo detección → priorización → takedown.

- **Unifica la visibilidad.** Dominios, redes sociales, dark web y señales internas en un solo tablero de riesgo. 360 Brand Guardian centraliza y prioriza hallazgos externos para que Riesgo, Marketing y Legal actúen en minutos.
- **Playbooks sin ambigüedades.** Roles, SLA y acciones claras para cada tipo de takedown. 360 Brand Guardian automatiza y orquesta solicitudes de baja; dashboards y workflows integrados reducen el "limbo" operativo.
- **Educación continua y segmentada.** Mensajes breves y repetitivos por región/amenaza. Los reportes y alertas de 360 Brand Guardian alimentan campañas de marketing/atención al cliente con amenazas reales y actuales.

Conclusión

El fraude digital está mutando hacia tácticas que explotan la confianza en la marca y se sostienen en canales externos difíciles de controlar. La primera mitad de 2025 demuestra que **actuar rápido donde más duele (phishing y suplantación de marca) y adaptar la respuesta por región** es clave para reducir pérdidas y preservar la relación con el cliente. Con **360 Brand Guardian**, puedes pasar de la reacción tardía a la **disrupción proactiva**: ver antes, bajar más rápido y comunicar con transparencia.

SOBRE APPGATE

Appgate asegura y protee los activos y aplicaciones más valiosos de una organización. Appgate es el líder del mercado en Zero Trust Network Access (ZTNA) y protección contra el fraude en línea. Los productos de Appgate incluyen Appgate ZTNA para ZTNA Universal y 360 Fraud Protection. Los servicios de Appgate incluyen análisis de asesoramiento sobre amenazas e implantación de ZTNA. Appgate protege a empresas y organismos públicos de todo el mundo. Más información en appgate.com.

appgate