CSIRT FINANCIERO | Aso Ban Caria

Memoria anual

2025

Fecha de publicación: Abril 2026

Tabla de Contenido

Prólogo

En un entorno donde la transformación digital avanza a un ritmo sin precedentes, las organizaciones del sector financiero enfrentan un panorama de amenazas cada vez más complejo, dinámico y persistente. Ya no solo se trata de responder a incidentes aislados, sino de incorporar una visión estratégica y de largo plazo que fortalezca la resiliencia institucional y promueva la anticipación como principio rector de la seguridad digital.

Durante el último año, hemos sido testigos de un cambio de paradigma: la aparición de amenazas avanzadas como el malware asistido por Inteligencia artificial y el modelo de Ransomware-as-a-Service, que han reducido los tiempos de ejecución de los adversarios y ampliado la superficie de exposición del sector. Fuentes públicas señalan que los actores maliciosos continúan explotando fraudes, ransomware y servicios vulnerables debido a la lentitud en las actualizaciones.

En 2025, Colombia enfrentó un entorno de amenazas complejo, con la presencia de grupos de ransomware, hacktivistas, brokers de acceso, actores estatales o proxy y ciberdelincuentes enfocados en fraude masivo. La atribución es un desafío, ya que como se menciona en diferentes estudios de ciberseguridad global, aproximadamente el 27% de los ataques no pueden relacionarse claramente con un actor específico, lo que incrementa la incertidumbre estratégica.

La evolución tecnológica trae consigo nuevos desafíos para las instituciones financieras, especialmente en el ámbito de la protección de identidades digitales y la seguridad en arquitecturas de nube híbrida. Estos aspectos requieren un enfoque proactivo y la implementación de soluciones avanzadas que permitan anticipar riesgos emergentes y garantizar la resiliencia operativa. Por ello, resulta fundamental adoptar una visión estratégica basada en estándares internacionales y buenas prácticas, Fomentando tanto la innovación como la gobernanza tecnológica. El fortalecimiento de la seguridad es un proceso continuo que demanda liderazgo, formación especializada y colaboración interinstitucional.

Este informe, lejos de ser un simple recuento de incidentes, se presenta como un testimonio de la resistencia y capacidad de adaptación de una de las infraestructuras críticas más representativas del país. Expone los riesgos enfrentados, así como el impacto potencial de la explotación de vulnerabilidades, y destaca la importancia de adoptar un proceso continuo de mejora, donde la seguridad digital es vista como un ciclo de adaptación permanente.

Por otro lado, un aspecto clave que se resalta es la cooperación interinstitucional, partiendo del principio de que la seguridad digital trasciende los límites de una sola organización y requiere la articulación efectiva entre equipos internos, dependencias técnicas y administrativas, proveedores estratégicos y entidades aliadas. El fortalecimiento de redes de confianza y la participación en entornos colaborativos permiten el intercambio ágil y seguro de información, la validación de buenas prácticas y una respuesta coordinada ante incidentes que afectan a múltiples actores del sector.

De igual forma, el reporte oportuno de incidentes se consolida como uno de los mecanismos más relevantes para la gestión integral del riesgo. Fomentar una cultura de reporte abierto y sin sesgos facilita la activación de procedimientos de respuesta, el desarrollo de estadísticas, la identificación de patrones y la anticipación frente a amenazas emergentes, reflejando la madurez organizacional y la capacidad de construcción de resiliencia sectorial. Otro aspecto fundamental, es fomentar una cultura de seguridad digital, pues sin la comprensión del papel individual en la protección del entorno digital, ninguna tecnología o control será suficiente. Por ello, resulta vital sensibilizar a los equipos, fortalecer hábitos seguros y promover la corresponsabilidad en todos los niveles de la organización, asegurando que la gestión esté alineada con los valores institucionales y las demandas del ecosistema actual.

Como resultado de este análisis, el Estado se viene preparando a través de acciones estratégicas, la Estrategia Digital busca defenderse de la IA maliciosa usando IA, el CONPES 4144 de 2025 establece el marco ético y legal para asegurar que el desarrollo y uso de esta tecnología en Colombia sea responsable y seguro, asimismo, la Estrategia Nacional de Seguridad Digital orienta sus objetivos hacia el fortalecimiento de la resiliencia frente a amenazas cibernéticas, la promoción de una cultura de seguridad digital en todos los niveles, y el desarrollo de capacidades técnicas y humanas para la prevención, detección y respuesta ante incidentes. Además, busca fomentar la cooperación público-privada y la articulación intersectorial, garantizando la protección de infraestructuras críticas y promoviendo la innovación segura en el ecosistema digital nacional. Estos objetivos son esenciales para consolidar un entorno digital confiable, sostenible y preparado para afrontar los retos emergentes del sector financiero y del país en su conjunto.

A su vez, la implementación de la Política de Seguridad Digital respaldada por un marco claro de gobernanza como el Decreto 338 de 2022, constituye un elemento indispensable para garantizar la protección de los activos de información, la continuidad operativa y el cumplimiento de las responsabilidades misionales del sector financiero. En este sentido, la colaboración entre las entidades que integran el CSIRT financiero, conformado por diversos bancos y actores estratégicos, es fundamental para blindar el motor financiero de Colombia y asegurar su confiabilidad ante los desafíos actuales y futuros.

Reafirmamos nuestro compromiso de acompañar al sector en cada etapa del ciclo de defensa e invitamos a todas las instituciones a fortalecer el trabajo conjunto, donde el riesgo se transforme en oportunidad de mejora y la seguridad digital sea el pilar del crecimiento sostenible y la confianza de la sociedad.

EQUIPO DE RESPUESTA A EMERGENCIAS CIBERNÉTICAS DE COLOMBIA
ColCERT - Ministerio TIC.

Resumen ejecutivo

Durante el 2025, el CSIRT Financiero de Asobancaria desempeñó un papel fundamental dentro del ecosistema de ciberseguridad del sector financiero, afianzando su operación y dando pasos firmes en la ejecución de su estrategia sectorial. El trabajo realizado estuvo enfocado, ante todo, en proteger la continuidad de los servicios financieros, apoyar a las entidades en la gestión de incidentes cibernéticos y fortalecer el trabajo conjunto entre los distintos actores del sector y otras instituciones clave.

En la operación diaria, el CSIRT Financiero de Asobancaria mantuvo un funcionamiento constante y confiable, atendiendo incidentes y eventos de ciberseguridad que afectaron o pudieron llegar a afectar a las entidades vinculadas al programa gremial. A lo largo del año, se realizaron ajustes y mejoras en los procesos de monitoreo, análisis y gestión de incidentes, lo que permitió ordenar mejor la atención de los casos, definir prioridades con mayor claridad y escalar oportunamente los eventos más críticos. Estos cambios se tradujeron en respuestas más ágiles y mejor coordinadas frente a incidentes y eventos de distinta naturaleza y nivel de impacto. De manera paralela, se avanzó en la organización y documentación de los procedimientos operativos, tomando como referencia buenas prácticas ampliamente utilizadas a nivel internacional.

El trabajo operativo se vio respaldado por un análisis permanente de amenazas y vulnerabilidades, así como por la emisión de alertas y comunicados dirigidos al sector financiero. La información compartida permitió que las entidades contaran con insumos oportunos para anticiparse a posibles riesgos y reforzar sus controles. Este enfoque ayudó a fortalecer una gestión

más preventiva del riesgo cibernético y a mantener al sector atento frente a nuevas modalidades de ataque que fueron apareciendo durante el año.

Desde una perspectiva estratégica, el CSIRT Financiero de Asobancaria enfocó sus esfuerzos en seguir fortaleciendo sus capacidades internas y en consolidar su posicionamiento como un referente para el sector en materia de ciberseguridad. En este sentido, se trabajó en la definición de líneas de acción orientadas a mejorar la madurez del servicio, optimizar los procesos existentes y fortalecer el equipo humano, reconociendo que la experiencia y el conocimiento especializado son claves para una respuesta efectiva ante incidentes.

Un aspecto relevante de la gestión durante 2025 fue el fortalecimiento de la coordinación y la colaboración. Se mantuvo un trabajo articulado y permanente con las entidades del sector financiero, promoviendo espacios de colaboración con grupos de ciberseguridad a nivel nacional e internacional, así como con entidades públicas y otros actores relevantes del ecosistema. Estos espacios fortalecieron el intercambio oportuno de información, mejoraron la coordinación ante incidentes de alcance sectorial y permitieron alinear capacidades y esfuerzos frente a desafíos comunes.

En línea con lo expuesto anteriormente, la información compartida a través de las instancias de Malware Information Sharing Platform (MISP) de INCIBE, FIRST y ColCERT resultó fundamental para la gestión del riesgo cibernético en el sector financiero. Por medio de este mecanismo, se difundieron indicadores de compromiso, alertas y contexto relevante sobre amenazas activas, lo que permitió a las entidades financieras contar con información oportuna y útil para reforzar sus controles y anticiparse a posibles incidentes. El uso permanente de MISP favoreció un intercambio más ágil y colaborativo, fortaleciendo la capacidad del sector para responder de manera coordinada frente a amenazas comunes.

Adicionalmente, se impulsaron actividades de capacitación, ejercicios y acciones de sensibilización dirigidas a las entidades del sector, con el objetivo de fortalecer su nivel de preparación y promover una cultura de ciberseguridad acorde con la importancia de los servicios financieros. Estas iniciativas contribuyeron a que la ciberseguridad fuera entendida no solo como un tema técnico, sino como una responsabilidad compartida.

En términos generales, la gestión desarrollada por el CSIRT Financiero durante el 2025 permitió avanzar de manera sólida y sostenida en el cumplimiento de su propósito. El trabajo realizado fortaleció de forma tangible la resiliencia cibernética del sector financiero y sentó bases firmes para afrontar los desafíos de un entorno digital cada vez más complejo, exigente y en constante evolución.

Atentamente,

Equipo del CSIRT Financiero

Resumen de servicios CSIRT Financiero

Comprometido con la mejora continua, el CSIRT Financiero realizó diversas investigaciones sobre ciberamenazas que, de forma directa o transversal, podrían haber impactado la infraestructura en Colombia, con especial enfoque en el sector bancario.

A través de servicios especializados, ha desarrollado y compartido productos diseñados para mitigar riesgos, fortalecer la seguridad del sector financiero y proteger a la comunidad bancaria del país.

Threat Intelligence **Prevention**

Este servicio está diseñado para identificar y anticipar posibles amenazas mediante un monitoreo proactivo y la recopilación de información estratégica. El CSIRT Financiero compartió 40 productos, los cuales ayudaron a las entidades del sector financiero a tomar decisiones informadas para prevenir incidentes de seguridad y mitigar los riesgos asociados con diversas ciberamenazas que impactaban la industria.

Strategy CTI Office:

Mediante un análisis consolidado de información mensual y trimestral, el CSIRT Financiero proporcionó tendencias clave y la evolución de las amenazas. Se compartieron 16 productos para ofrecer una visión detallada sobre el panorama de ciberamenazas que afectaron directa o indirectamente al sector financiero en Colombia.

APT monitor & analysis Impact:

A partir del seguimiento y análisis de las principales amenazas persistentes avanzadas (APT), incluyendo actores, modus operandi y técnicas, el CSIRT Financiero elaboró 24 productos enfocados en estos grupos de amenazas que podrían poner en riesgo la infraestructura tecnológica en Colombia.

Threat Intelligence **RESPONSE**

Orientado a analizar, responder y mitigar eventos o incidentes de ciberseguridad en tiempo real, proporcionando información y acciones específicas para contener las amenazas de manera efectiva. A través de este servicio, el CSIRT Financiero compartió más de 1.350 productos, facilitando la identificación de cadenas de infección utilizadas por actores maliciosos y sus respectivas familias de malware.

Threat Analysis & Modeling:

Analizando eventos de seguridad, actores de amenazas, malware, arquitecturas y vulnerabilidades, el CSIRT Financiero compartió 977 productos que facilitaron la identificación de patrones y comportamientos de amenazas que podrían estar dirigidas o tener alguna incidencia sobre la infraestructura tecnológica de los asociados.

Advanced Threat Emulation:

Simulando las actividades de los actores de amenazas mediante la ejecución controlada de malware, se entregaron 4 productos (2 Malware Emulation y 2 Endpoint Analysis) que permitieron replicar el comportamiento de las amenazas y generar medidas de detección, con el objetivo de fortalecer las capacidades de contención y mitigación dentro de las entidades asociadas.

Threat Security Response:

A través del conocimiento, los procesos y las acciones necesarias para una respuesta efectiva ante eventos o incidentes de seguridad, el CSIRT Financiero desarrolló y entregó 10 productos en los que se incluye: casos de uso de amenazas (Threat Use Cases), manuales de respuesta a incidentes (Incident Response Playbooks) y estrategias de mitigación. Además, a través del subservicio Support Incident Response, se gestionaron 363 reportes relacionados con phishing, distribución de malware, suplantación de aplicaciones y abuso de marca.

Threat Detection & Prevent:

Mediante inteligencia de amenazas aplicable en infraestructuras de seguridad y equipos de “Blue Team”, el CSIRT Financiero compartió 38 productos relacionados a reglas YARA y SIGMA, fortaleciendo así las capacidades de defensa adaptativa ante amenazas dirigidas posiblemente al sector financiero en Colombia.

Resúmenes entregables CSIRT Financiero

El CSIRT Financiero a través de sus servicios y subservicios compartió más de 1.400 productos y más de 24.000 indicadores de compromiso, como resultado de las investigaciones realizadas sobre las distintas ciberamenazas que afectaron o pudieron tener incidencia en el sector financiero en Colombia durante el 2025.

12	Security Bulletins (SB):
4	Strategy Bulletins (STRB)
24	Relevant Events (RE)
725	Cyber Security Warning (CSW)
51	Tailored Threat Analysis - AGL
7	Tailored Threat Analysis - ASL
19	Tailored Threat Analysis - IoC
127	Tailored Threat Analysis - TMP
39	Vulnerability Threat Monitoring (VTM)
4	Monitoring Threat Analysis (MTA)
5	Threat Focus Report (TFR) / Monographic
2	Malware Emulation (ME)
2	Endpoint Analysis (EA)
3	Threat Use Cases (TUC)
5	Incident Response Playbooks (IRP)
2	Mitigation (MT)
363	Support Incident Response (SIR)
20	Malware Activity - YARA (MA)
18	Unified Threat Identification - Sigma (UTI)
13	Training hands-on (Webinars)

24.982	Indicadores de Compromiso

Gráfica 1. Resúmenes entregables CSIRT Financiero. Fuente: CSIRT Financiero.

Panorama global de ciberamenazas en Colombia 2025

En 2025, Colombia terminó de entender una verdad que durante años se había ignorado o subestimado: el riesgo digital no era un asunto exclusivo de los equipos de tecnología. Fue el año en que las ciberamenazas dejaron de percibirse como invisibles y pasaron a tener efectos reales, tangibles y costosos sobre empresas, instituciones públicas y servicios esenciales. Desde entonces, la ciberseguridad dejó de ser un tema operativo y se convirtió en un asunto estratégico.

El país hizo parte de un escenario global complejo. A nivel mundial, los ataques cibernéticos crecieron en frecuencia, impacto y sofisticación. La digitalización acelerada, la dependencia de proveedores tecnológicos y la interconexión entre organizaciones crearon un entorno ideal para los atacantes. Colombia, por su ritmo de transformación digital y su posición regional, quedó expuesta de manera directa y transversal.

Durante 2025, Colombia fue uno de los países más atacados de América Latina. No porque fuera el más débil, sino porque se volvió más visible. Más servicios en línea, más datos circulando, más sistemas conectados. La superficie de ataque creció más rápido que la capacidad de muchas organizaciones para protegerse.

Los ataques no se concentraron en un solo sector. Bancos, entidades públicas, empresas de servicios, industrias, universidades y pequeñas empresas fueron blanco constante. El mensaje fue contundente:

el tamaño ya no ofrecía protección. Estar conectado era suficiente para ser objetivo.

En ese contexto, muchas organizaciones entendieron tarde que la pregunta correcta no era si podían evitar todos los ataques, sino si estaban preparadas para resistirlos y recuperarse.

El ransomware fue, sin duda, una de las amenazas más determinantes del año. Este tipo de ataques no solo cifró información, sino que secuestró operaciones completas y puso a las organizaciones frente a decisiones difíciles, muchas veces bajo presión y sin margen de error.

Colombia enfrentó ataques de ransomware que afectaron directamente a empresas locales, desde compañías medianas hasta proveedores clave de servicios. En varios casos, los sistemas críticos quedaron inutilizados durante días, la facturación se detuvo y la operación diaria se paralizó. El impacto no fue solo técnico: fue financiero, reputacional y estratégico.

Además, el ransomware evolucionó. Ya no se trató únicamente de bloquear el acceso a la información, sino de amenazar con publicarla. La llamada doble extorsión aumentó el nivel de presión. Las organizaciones no solo temieron perder datos, sino también la confianza de clientes, aliados y ciudadanos.

La lección fue clara y dura: no contar con respaldos, planes de respuesta y liderazgo en crisis tuvo consecuencias reales. En muchos casos, el costo de no haber invertido antes fue mucho mayor que cualquier inversión preventiva.

Uno de los aprendizajes más estratégicos de 2025 fue entender que muchos ataques no llegaron de frente, sino por los costados. Los ataques a la cadena de suministro digital comenzaron a afectar a Colombia de forma silenciosa, pero profunda.

Empresas con buenos controles internos se vieron impactadas no porque fallaran directamente, sino porque uno de sus proveedores, plataformas o servicios

externos fue comprometido. Un solo eslabón vulnerable fue suficiente para afectar a múltiples organizaciones al mismo tiempo.

Este tipo de ataques dejó en evidencia una realidad incómoda: la seguridad de una organización ya no dependía solo de sí misma. Dependía también de la seguridad de sus aliados, proveedores tecnológicos y terceros críticos.

En sectores como el financiero, energético, educativo y el comercial, esta dependencia se volvió evidente. El riesgo ya no estaba solo dentro de la empresa, sino en todo el ecosistema que la sostenía.

El mensaje estratégico fue contundente: **la ciberseguridad dejó de ser individual y pasó a ser colectiva.**

Aunque la tecnología jugó un papel clave, muchos de los incidentes más graves de 2025 comenzaron con errores simples: un correo abierto sin verificar, una contraseña débil, una urgencia mal interpretada. La ingeniería social siguió siendo una de las herramientas más efectivas de los atacantes.

Esto dejó una conclusión difícil de ignorar: las personas siguieron siendo uno de los puntos más vulnerables, pero también podían ser una de las mejores defensas si contaban con la formación y la cultura adecuadas.

Top vectores de ataque observados en 2025

ENERO

Phishing	60%
Vulnerability	31%
Watering Hole	5%
Spearphishing	3%
Spoofing	1%

FEBRERO

Phishing	73%
Vulnerability	20%
Spearphishing	4%
Spoofing	2%
Man in The Middle	1%

MARZO

Phishing	61%
Vulnerability	30%
Spearphishing	5%
Spam	3%
Smishing	1%

ABRIL

Phishing	65%
Vulnerability	26%
Spam	5%
Remote Code Execution	3%
Smishing	1%

MAYO

Phishing	60%
Vulnerability	19%
Spam	9%
Watering Hole	8%
Remote Code Execution	4%

JUNIO

Phishing	53%
Vulnerability	33%
Remote Code Execution	9%
Spearphishing	5%

1 2 3 4 5 6

JULIO		AGOSTO		SEPTIEMBRE		OCTUBRE		NOVIEMBRE		DICIEMBRE	
Phishing	64%	Phishing	58%	Phishing	76%	Phishing	68%	Phishing	50%	Phishing	56%
Vulnerability	20%	Vulnerability	26%	Vulnerability	12%	Vulnerability	21%	Vulnerability	35%	Vulnerability	29%
Credential Theft	7%	Spam	7%	Watering Hole	4%	Remote Code Execution	7%	Spam	5%	Remote Code Execution	6%
Watering Hole	5%	Watering Hole	5%	Remote Code Execution	4%	Suplantación APP	2%	Remote Code Execution	5%	Spearphishing	5%
Spam	4%	Spearphishing	4%	Spearphishing	4%	Spearphishing	2%	Spearphishing	5%	Zero Day	4%

Gráfica 2. Top de vectores de ataques 2025. Fuente: CSIRT Financiero.

Threat Intelligence Response

Este servicio está orientado a la inteligencia de amenazas y al análisis de riesgos como soporte clave para la respuesta y corrección tanto estratégica como operativa. A través de la correlación de información técnica, contextual y de negocio, este enfoque permite priorizar acciones, contener incidentes de manera oportuna y reducir el impacto de las amenazas sobre los activos críticos. Asimismo, facilita la toma de decisiones informadas, el fortalecimiento de los controles de seguridad y la mejora continua de las capacidades de respuesta ante incidentes de ciberseguridad.

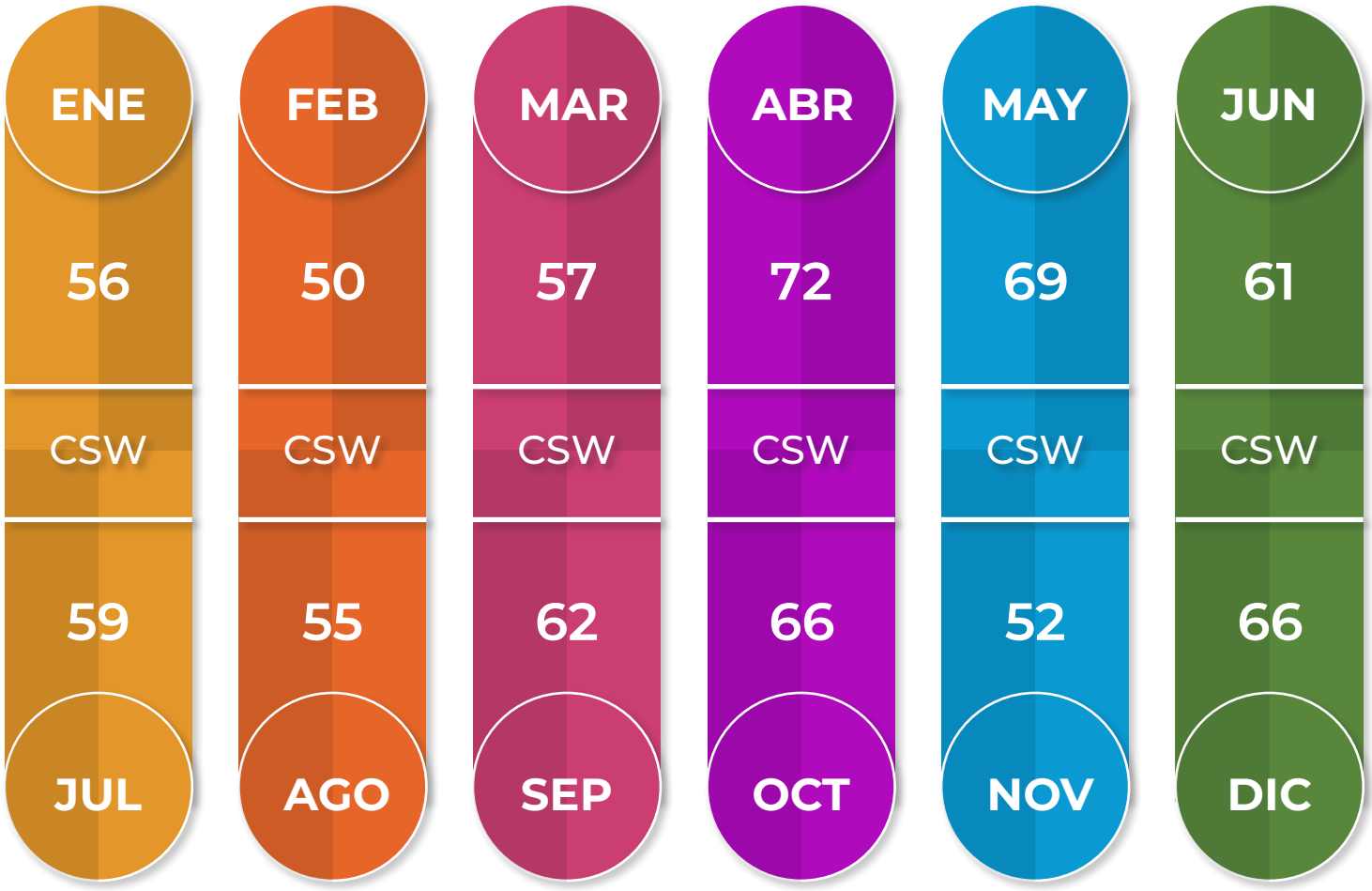
Threat Analysis & Modeling

El subservicio de Threat Analysis & Modeling tiene como objetivo proporcionar inteligencia de amenazas oportuna, contextualizada y accionable, orientada a fortalecer las capacidades de prevención, detección y respuesta frente a los riesgos cibernéticos que impactan al sector financiero. A través de este subservicio, se desarrollan distintos productos que permiten abordar el panorama de amenazas desde una visión integral, combinando alertas tempranas, análisis técnico profundo y monitoreo continuo.

Cyber Security Warning (CSW):

Durante 2025, el CSIRT Financiero emitió un total de 725 CSW, correspondientes a alertas diarias orientadas a informar oportunamente sobre amenazas cibernéticas relevantes. Estas alertas abarcaron un amplio espectro de riesgos que impactan al sector financiero, tanto a nivel local como global, permitiendo a las áreas involucradas anticiparse a posibles escenarios de ataque, fortalecer sus controles de seguridad y apoyar la toma de decisiones informadas. La generación constante de estos CSW refleja el compromiso del CSIRT Financiero con la vigilancia continua del panorama de amenazas y con la protección de la información y los activos críticos de las entidades.

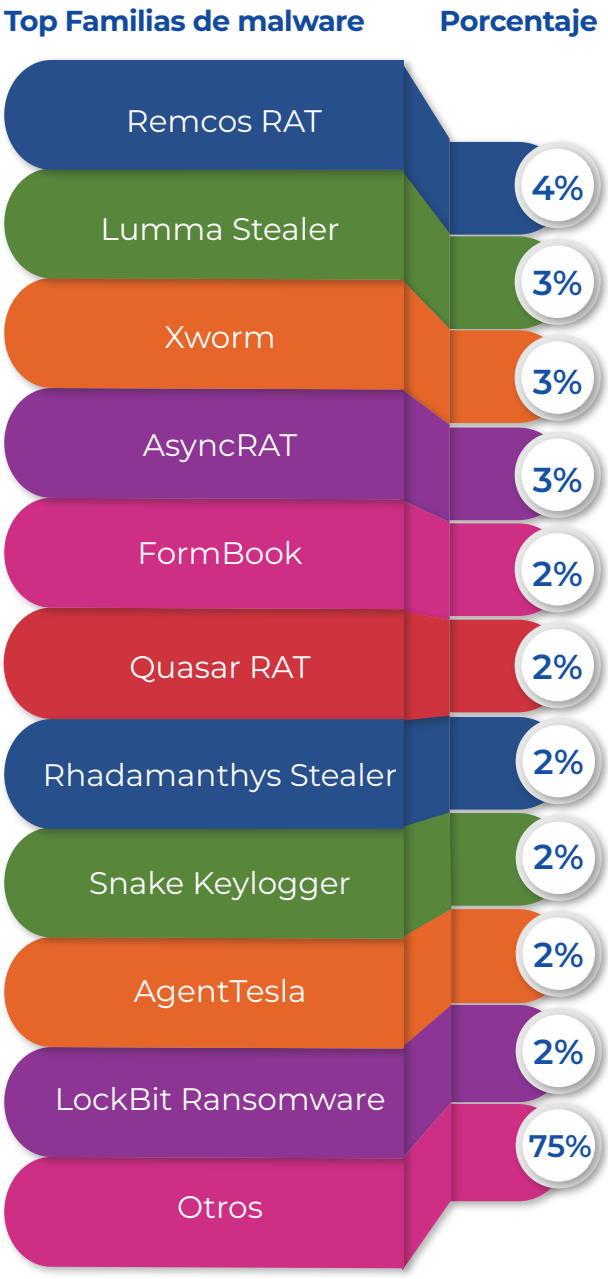
Cyber Security Warning reportadas en 2025



Gráfica 3. Cantidad de Cyber Security Warning reportadas. Fuente: CSIRT Financiero.

Dentro de las familias de malware identificadas en las CSW, se destacan principalmente los troyanos de acceso remoto (RAT) y los malware de tipo stealer, cuyo objetivo es obtener control no autorizado de los sistemas comprometidos y la exfiltración de información confidencial. Estas amenazas representan un riesgo significativo para la seguridad de los activos digitales, especialmente por su capacidad de facilitar el espionaje, la captura de credenciales y el acceso persistente a los entornos afectados. En la siguiente gráfica se presenta el top 10 de las familias de malware más observadas en los reportes de amenazas.

Familias de malware más observadas en las Cyber Security Warning



Gráfica 4. Principales familias de malware observadas en CSW reportadas 2025.
Fuente: CSIRT Financiero.

Tailored Threat Analysis (TTA):

Durante 2025 se elaboraron un total de 244 TTA, correspondientes a alertas especializadas orientadas al análisis de amenazas cibernéticas. Estos análisis permitieron evaluar de manera detallada malware, actores de amenaza, vulnerabilidades y riesgos emergentes, proporcionando inteligencia contextualizada y accionable para el sector financiero. La generación de estas TTA fortaleció la capacidad de anticipación y respuesta frente a amenazas sofisticadas, apoyando la toma de decisiones estratégicas y la mejora continua de los controles de ciberseguridad.

Las TTA se estructuran en diferentes modalidades, diseñadas para abordar el análisis de amenazas desde distintos enfoques y niveles de impacto, de acuerdo con su alcance, contexto y objetivo. Cada una de estas modalidades ofrece inteligencia especializada y accionable para el sector financiero.

Tailored Threat Analysis (TTA) realizadas durante 2025

Gráfica 5. Cantidad de Tailored Threat Analysis realizadas. Fuente: CSIRT Financiero.

Monitoring Threat Analysis / Advanced Threat Report (MTA)

Este producto está diseñado para el monitoreo continuo del entorno de amenazas, con enfoque en la identificación y el seguimiento de actividades maliciosas casi en tiempo real. Emplea diversas fuentes de información y herramientas de monitoreo para detectar patrones, campañas activas y comportamientos anómalos.

Gráfica 6. MTA realizados en 2025. Fuente: CSIRT Financiero.

Este es un producto analítico de carácter estratégico que aborda en profundidad una amenaza específica, examinando sus tácticas, técnicas y procedimientos (TTP), así como su evolución y posible impacto en las organizaciones. Este producto permite una comprensión integral de amenazas relevantes y emergentes.

Gráfica 7. TFR realizados en 2025. Fuente: CSIRT Financiero.

Threat Security Response

Threat Use Cases

El CSIRT Financiero desarrolla el entregable Threat Use Cases, el cual es un producto clave para operacionalizar la inteligencia de amenazas, transformando escenarios de ataque realistas en capacidades concretas de detección, análisis y respuesta a incidentes.

Estos casos de uso permiten identificar de forma proactiva las tácticas, técnicas y procedimientos (TTP) de los adversarios, optimizando los tiempos de detección y respuesta, estandarizando la actuación ante amenazas recurrentes o emergentes y facilitando la validación de las capacidades defensivas a lo largo de las fases del Cyber Kill Chain, fortaleciendo la identificación temprana y la prevención de acciones maliciosas en su infraestructura tecnológica.

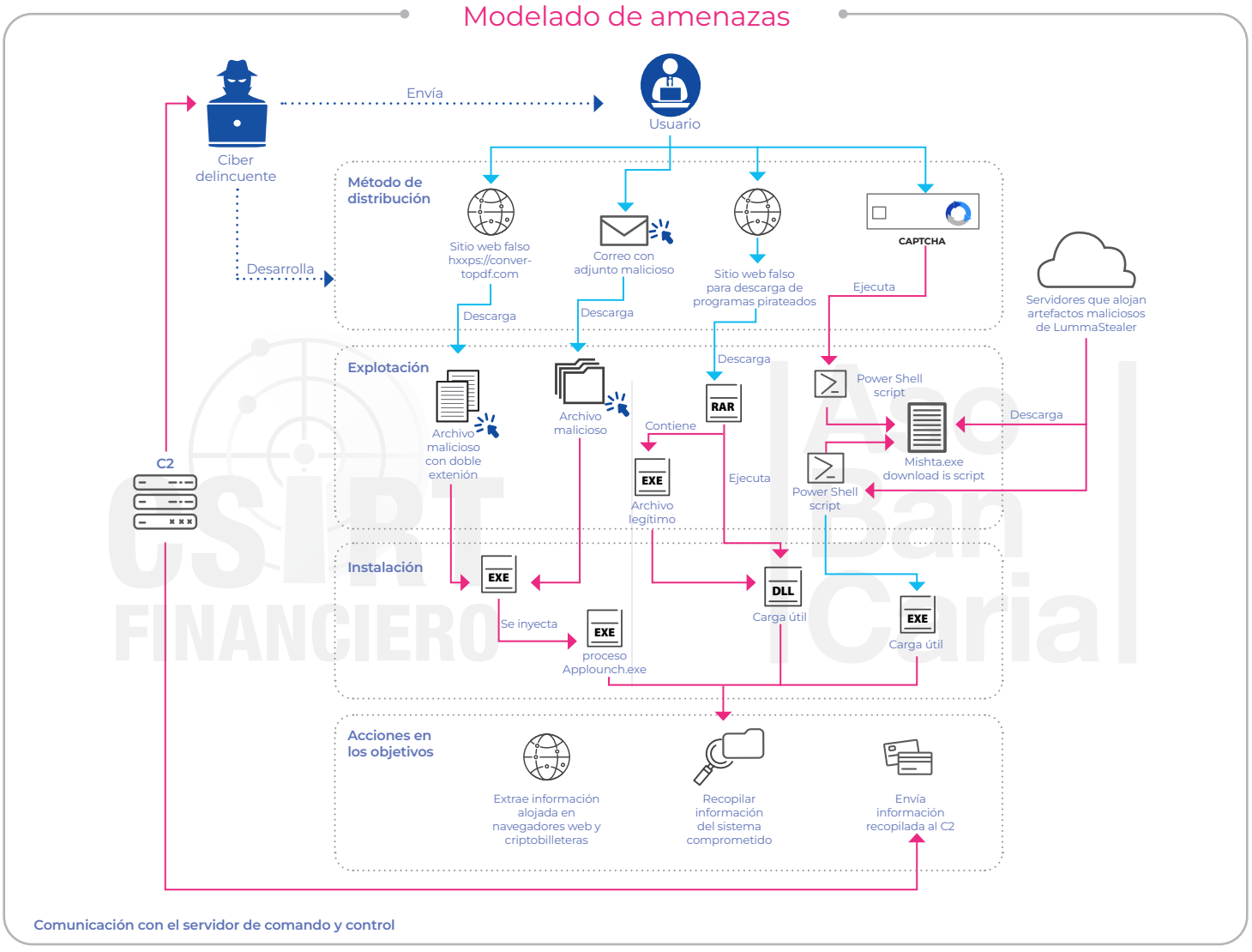
Para el año 2025 el CSIRT Financiero generó cuatro entregables asociados a diversas familias de malware, destacando a Lumma Stealer, Remcos RAT y FormBook, así como un kit de Phishing-as-a-Service (PhaaS). A través de estos productos se definieron medidas técnicas orientadas a la detección, contención y mitigación de dichas amenazas. A continuación, se presenta un resumen de los casos de uso desarrollados.

- Caso de uso para la detección, mitigación y contención de la amenaza Lumma Stealer (CRT-TUC-2025: marzo 2025).

  Lumma Stealer es un stealer que registró un aumento significativo en el año 2025 en Colombia, presentando constantes actualizaciones y diversos métodos de distribución siendo un riesgo para las organizaciones de todos los sectores, entre ellos el financiero.

  Entre sus capacidades destaca la recopilación de información de navegadores basados en Chromium como Chrome, Edge, Opera, Brave, entre otros, y Mozilla (Firefox, Waterfox, entre otros), así como de alrededor de 70 extensiones de criptomonedas y 2FA.

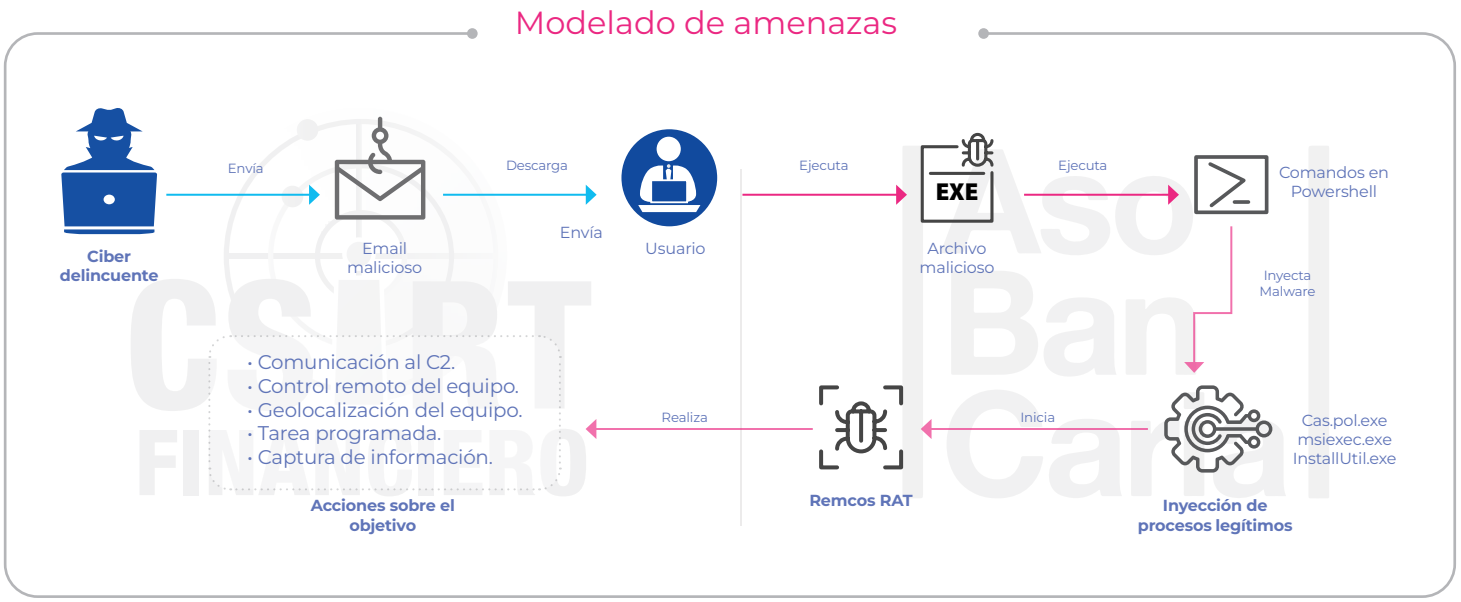
A continuación, se presenta el modelado del evento basado en las campañas vistas por el CSIRT Financiero:



Gráfica 8. Modelado de la amenaza Lumma Stealer. Fuente: CSIRT Financiero.

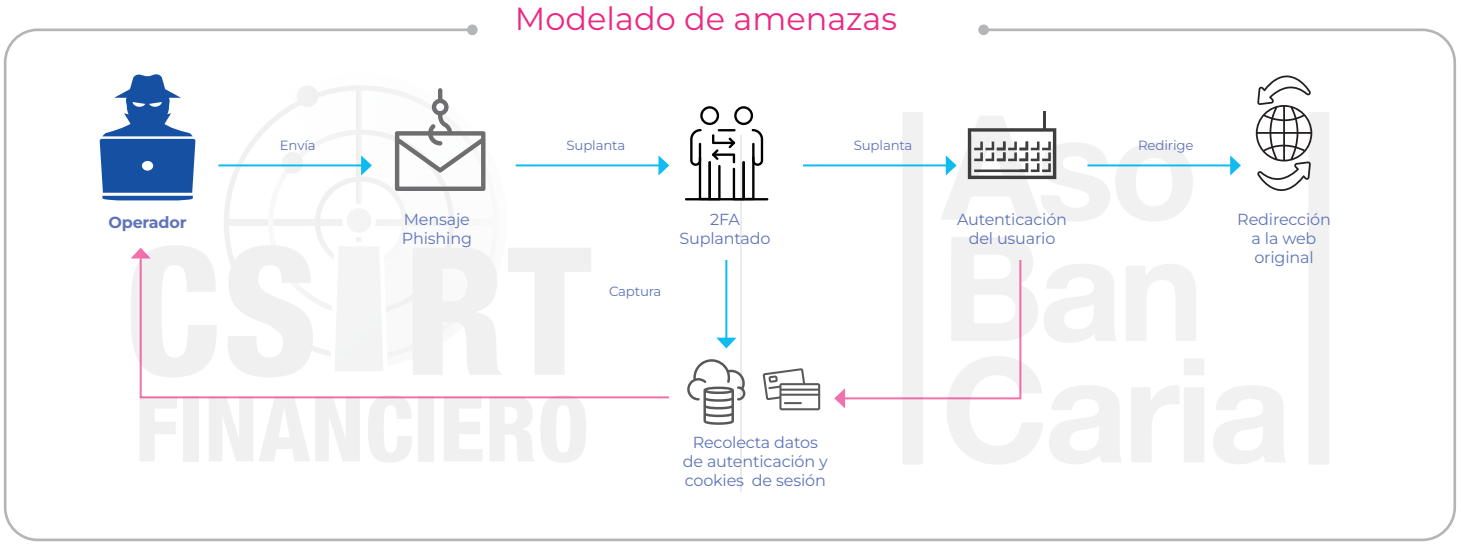
- Caso de uso para la detección, mitigación y contención del troyano de acceso remoto Remcos (CRT-TUC-2025-002: junio 2025).

Remcos es un Troyano de Acceso Remoto (RAT) comercial utilizado por ciberdelincuentes para tomar control total de los sistemas comprometidos de forma remota. Aunque fue diseñado inicialmente como una herramienta legítima de administración remota, ha sido ampliamente adoptado en campañas maliciosas.



Gráfica 9. Modelado de la amenaza Remcos RAT. Fuente: CSIRT Financiero.

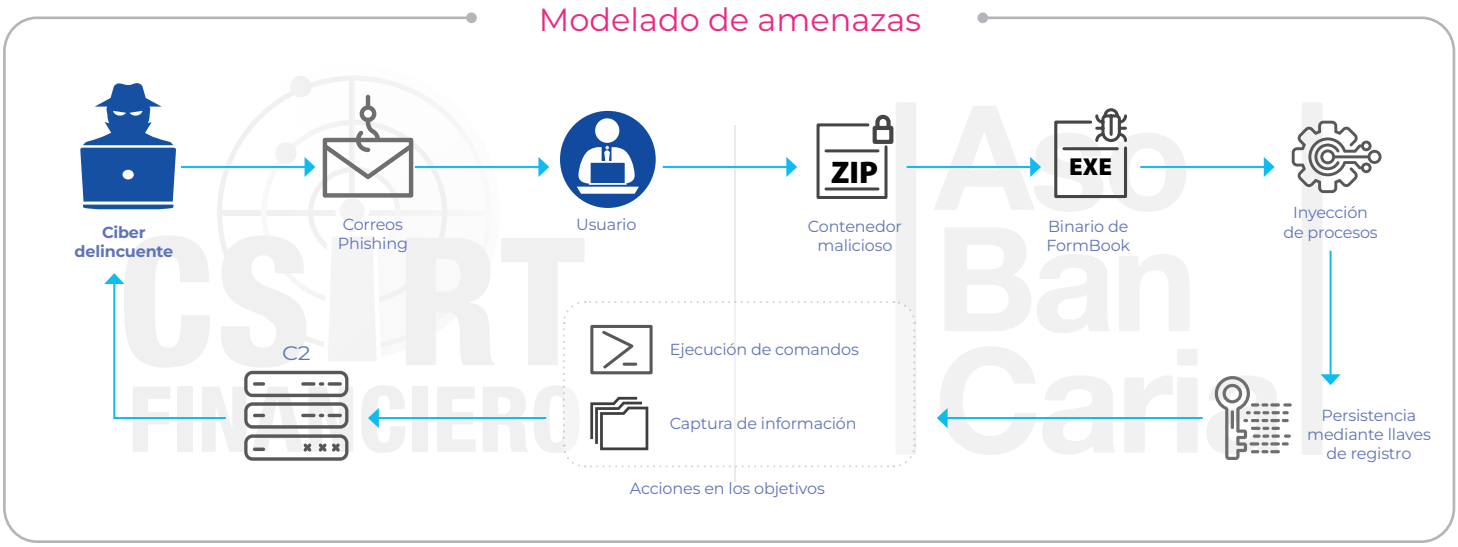
- Casos de uso para la detección, mitigación y contención de la amenaza Tycoon 2FA (CRT-TUC-2025-003: septiembre 2025).



Gráfica 10. Modelado de la amenaza Tycoon 2FA. Fuente: CSIRT Financiero.

- Caso de uso para la detección, mitigación y contención de FormBook (CRT-TU-2025-004: diciembre 2025)

Luego de analizar diversas campañas de FormBook, se desarrolló la siguiente gráfica en el que se presenta un modelado de los eventos analizados:



Gráfica 11. Modelado de la amenaza FormBook. Fuente: CSIRT Financiero.

Incident Response Playbook

El Incident Response Playbook corresponde a un producto técnico desarrollado por el CSIRT Financiero que establece un conjunto estructurado de procedimientos operativos para la gestión de incidentes de ciberseguridad específicos. Dichos procedimientos han sido definidos y organizados conforme al framework del NIST, el cual se ha utilizado como referencia para determinar las fases del ciclo de respuesta a incidentes, abarcando desde la detección y análisis inicial, hasta las etapas de contención, erradicación, recuperación y actividades post-incidente. Este producto define de manera clara los criterios de activación, los roles y responsabilidades de los equipos involucrados, así como las acciones técnicas y de coordinación que deben implementarse frente a cada escenario de incidente.

Asimismo, este entregable proporciona un marco estandarizado que permite reducir los tiempos de respuesta, minimizar el impacto operativo y asegurar la consistencia en la actuación de los equipos de respuesta a incidentes, facilitando la toma de decisiones bajo condiciones de alta presión. Su diseño contempla la integración

con capacidades de monitoreo, detección y orquestación, así como la incorporación de lecciones aprendidas, contribuyendo a la mejora continua de la capacidad de respuesta a incidentes y al fortalecimiento de la madurez operativa de la organización.

Durante el 2025 se realizaron cuatro Incident Response Playbook:

- Actualización: defensa ante amenazas de tipo RAT (CRT-IRP-2025-001: abril 2025).
- Compromiso de Cuentas - Account Takeover (CRT-IRP-2025-002: abril 2025)
- Mecanismos de persistencia (CRT-IRP-2025-003: mayo 2025).
- Compromiso en cadena de suministro (CRT-IRP-2025-004: octubre 2025).

Support Incident Response

El servicio de Support Incident Response (SIR) es el conjunto de actividades de apoyo técnico, analítico y organizacional generado por el CSIRT Financiero que respalda la respuesta a posibles incidentes y eventos de seguridad presentados en las infraestructuras tecnológicas y que son reportados por los asociados.

De las solicitudes atendidas, el CSIRT Financiero analizó e identificó correos tipo phishing y Spearphishing, archivos maliciosos relacionados con malware, suplantación de sitios o aplicaciones web, credenciales comprometidas, entre otras situaciones.

Nuestro objetivo como CSIRT Financiero es facilitar, acelerar y mejorar la efectividad del proceso de respuesta a incidentes, asegurando que los equipos responsables cuenten con la información, herramientas, coordinación y contexto necesarios para actuar de forma oportuna y controlada.

Durante 2025 se atendieron 363 eventos de ciberseguridad a través del servicio Support Incident Response, los cuales están distribuidos así:

Volumen de eventos de ciberseguridad por mes

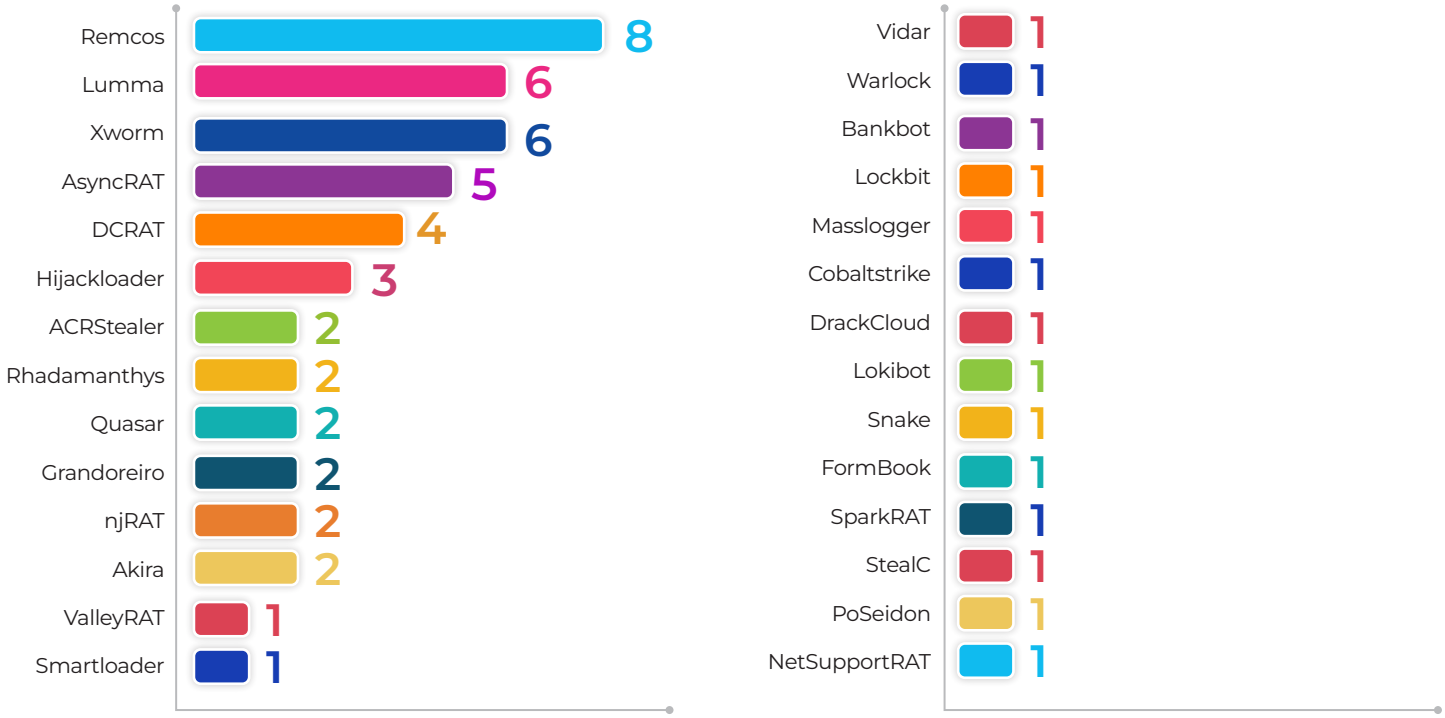
Gráfica 12. Volumen de eventos de ciberseguridad por mes. Fuente: CSIRT Financiero.

Familias de malware obtenidas de los Support Incident Response

Mediante estas investigaciones, se obtuvo información muy valiosa sobre las diferentes familias de malware que están afectando de forma directa al sector financiero colombiano a través de los incidentes/eventos reportados por nuestros asociados.

En la siguiente gráfica se observa que Remcos RAT, Xworm, Lumma Stealer y AsyncRAT fueron las familias de malware más recurrentes durante lo corrido del año 2025.

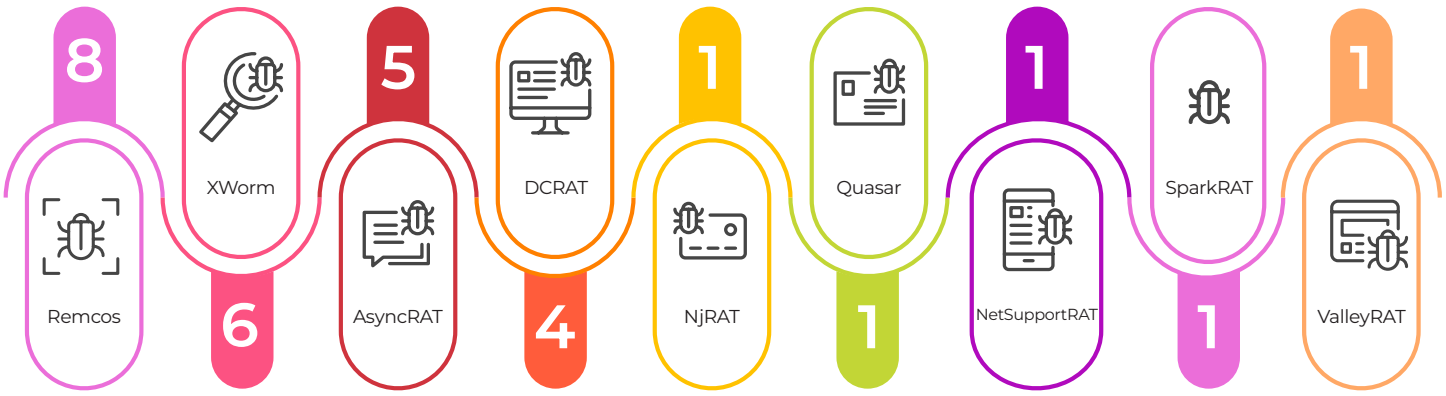
Familias de malware observadas en incidentes/eventos reportados



Gráfica 13. Familias de malware identificadas en 2025. Fuente: CSIRT Financiero.

Por otro lado, al agrupar la información por familias de malware, se evidenció la predominancia de Troyanos de Acceso Remoto (RAT), lo que refleja un interés sostenido de los actores de amenaza en obtener y mantener acceso remoto persistente a los sistemas comprometidos, con el objetivo de sostener compromisos prolongados, discretos y de baja visibilidad.

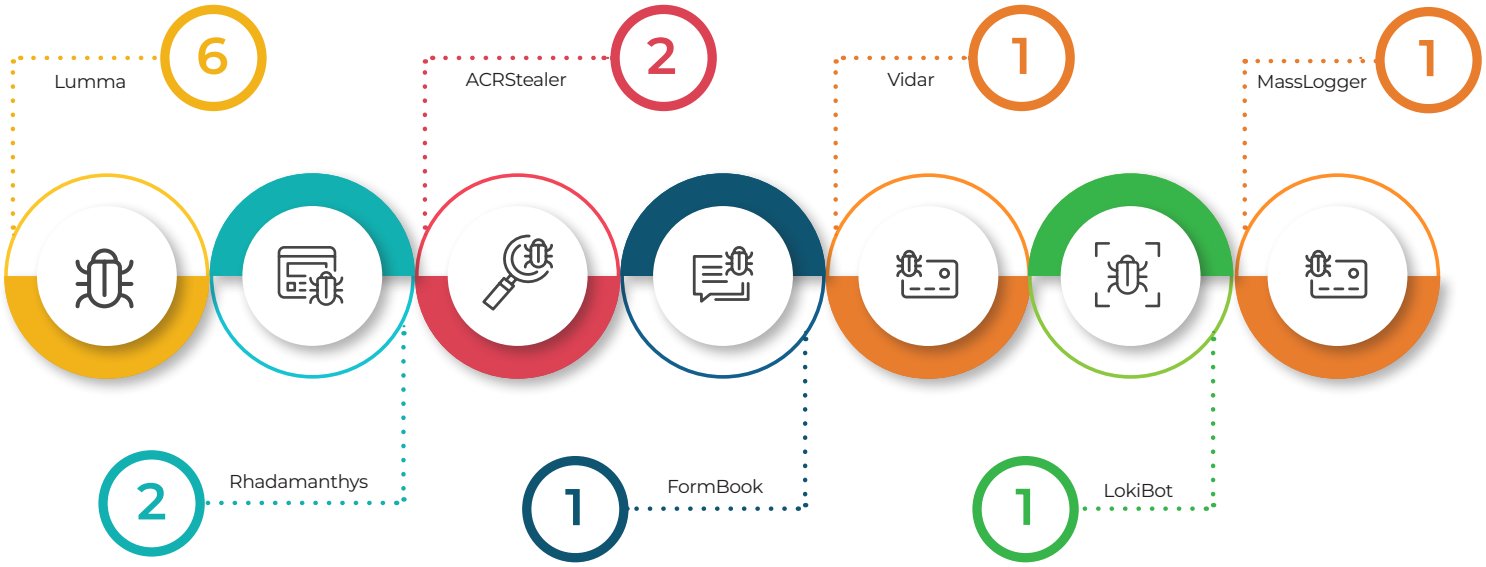
Malware de tipo RAT identificado



Gráfica 14. Malware de tipo RAT identificado en los Support Incident Response. Fuente: CSIRT Financiero.

Otra de las familias de malware observada son los stealers o infostealers. Se evidenció un objetivo claro por parte de los actores cibercriminales orientado a la obtención de información sensible, en particular credenciales bancarias. Este tipo de información permite a los actores maliciosos ejecutar actividades ilícitas posteriores, tales como fraude financiero, apropiación indebida de cuentas y abuso de servicios, incrementando de forma significativa el riesgo para las organizaciones afectadas.

Malware de tipo stealer identificado



Gráfica 15. Malware de tipo stealer identificado en los Support Incident Response. Fuente: CSIRT Financiero.

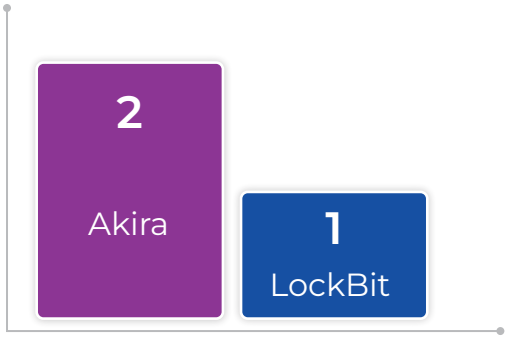
En menor proporción, se identificó malware de tipo loader, utilizados principalmente como vector de infección de primera etapa, con la capacidad de facilitar la entrega de cargas maliciosas adicionales y escalar hacia campañas más complejas y estructuradas.

Malware de tipo loader identificado

Gráfica 16. Malware de tipo loader identificado en los Support Incident Response. Fuente: CSIRT Financiero.

Si bien el ransomware se presenta con menor frecuencia, su impacto sobre las organizaciones es significativamente elevado, representando un riesgo crítico para la continuidad operativa.

Malware de tipo ransomware identificado



Gráfica 17. Ransomware identificado.
Fuente: CSIRT Financiero

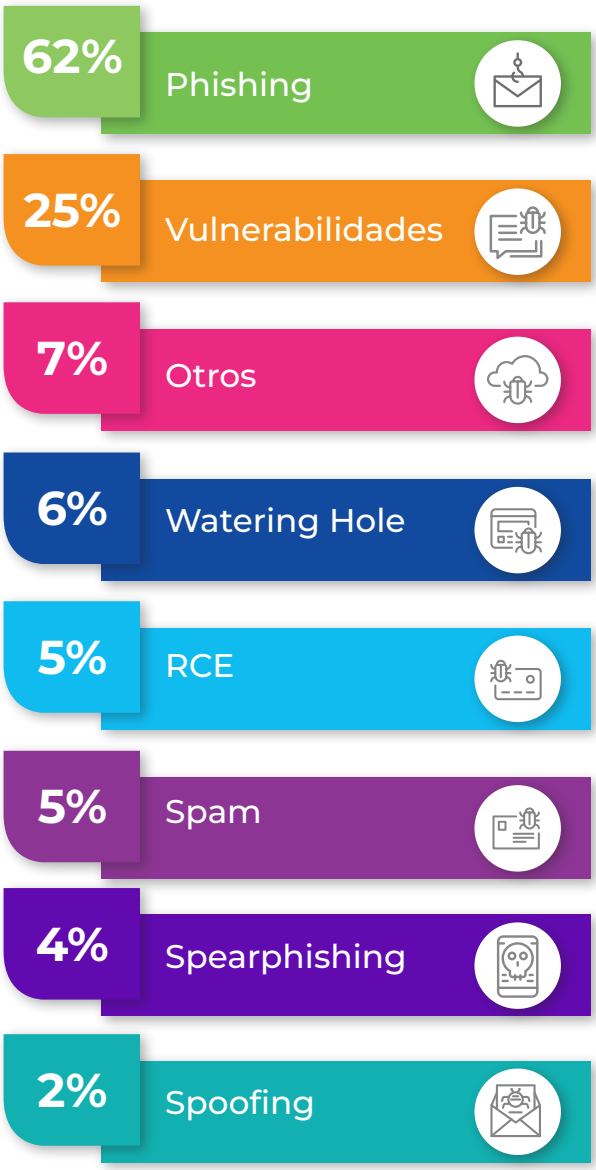
Vectores de ataque

En relación con los vectores de ataque, se evidenció que el phishing se consolidó como el vector dominante, liderando de forma consistente en todo 2025, con un promedio cercano al 62%. Este comportamiento confirma la necesidad de fortalecer los controles preventivos, así como mantener programas permanentes de concienciación y capacitación orientados a reducir la exposición de los usuarios frente a este tipo de amenazas.

En segundo lugar, se observó una alta recurrencia en la explotación de vulnerabilidades, poniendo de manifiesto la importancia de una gestión continua de actualizaciones y parches en la infraestructura tecnológica, como medida clave para reducir la superficie de ataque y mitigar riesgos de compromiso.

A continuación, se presenta el promedio para todos los vectores de ataque observados mediante el reporte de los Support Incident Response:

Vectores de ataque utilizados por ciberdelincuentes



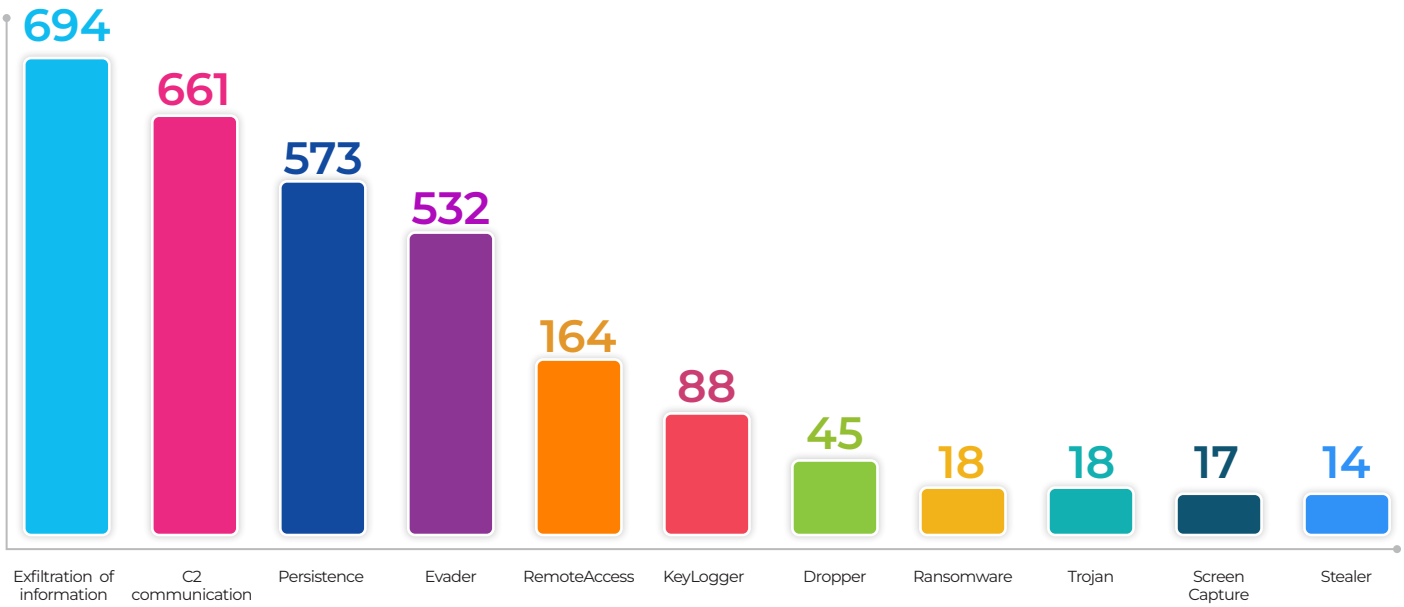
Gráfica 18. Vectores de ataque utilizados.
Fuente: CSIRT Financiero

Capacidades

El análisis de las capacidades maliciosas observadas evidencia que las amenazas identificadas se orientan principalmente a la exfiltración de información y al establecimiento de canales de comunicación con infraestructuras de comando y control (C2), lo que refleja interés de los actores maliciosos en el robo de datos y el control persistente de los sistemas comprometidos.

Asimismo, se observa una alta presencia de técnicas de persistencia y evasión, lo que indica campañas diseñadas para permanecer de forma prolongada y operar de manera sigilosa dentro de los entornos afectados. En menor medida, se identifican capacidades asociadas al acceso remoto, registro de pulsaciones de teclado y captura de pantalla, reforzando el enfoque en la obtención de información sensible, mientras que el ransomware, aunque menos frecuente, representa un riesgo de alto impacto operativo para las organizaciones.

Capacidades utilizadas por los ciberdelincuentes



Gráfica 19. Capacidades identificadas en 2025. Fuente: CSIRT Financiero.

Asimismo, como resultado de la actividad de monitoreo en la Deep y Dark Web, se identificaron cuentas comprometidas de colaboradores y clientes de distintas entidades financieras, las cuales fueron reportadas y consolidadas en 201 productos, representando más de la mitad de los Support Incident Response reportados durante el 2025.

Mitigations

Las mitigaciones corresponden a un conjunto de controles y medidas defensivas que están diseñadas para ayudar a los asociados a reducir la probabilidad y el impacto de un ciberataque, basándose en el comportamiento real de los adversarios.

Este tipo de entregables proporcionan una guía práctica para fortalecer las capacidades de prevención, contención y resiliencia frente a las diferentes ciberamenazas. Su adopción facilita la identificación de brechas, la evaluación objetiva de la madurez de seguridad y el fortalecimiento de la postura defensiva de las organizaciones, apoyando tanto la gestión de riesgos como la toma de decisiones.

Las mitigaciones constituyen un insumo clave para contener incidentes en curso, reducir la superficie de ataque y mejorar la capacidad de respuesta ante amenazas recurrentes o avanzadas.

En 2025 se elaboraron dos mitigaciones orientadas:

- M1015 – Active Directory Configuration (CRT-MT-2025-001: mayo 2025) presenta bases sólidas orientadas a una adecuada configuración del Directorio Activo. La implementación de esta mitigación permite reducir significativamente los riesgos asociados a este componente crítico de la infraestructura tecnológica, contribuyendo al fortalecimiento y protección de Active Directory frente a modificaciones maliciosas, debilidades en la configuración y posibles abusos que podrían facilitar el escalamiento de privilegios, la persistencia de actores maliciosos o incluso la toma de control del dominio.

- M1054 – Software Configuration (CRT-MT-2025-002: octubre 2025) presenta de manera práctica y accionable los métodos de detección para todas las técnicas vinculadas a esta mitigación; articulando para cada técnica un mapa claro que enlaza fuentes de telemetría, reglas de correlación y criterios de priorización objetiva, de forma que los equipos de detección puedan traducir hallazgos en alertas de alta fidelidad.

Threat Detection & Prevent

Malware Activity

Una regla YARA es una definición de detección que combina patrones (texto o binario) con una condición lógica para identificar archivos que coincidan con una amenaza; opcionalmente puede incluir metadatos para aportar contexto y trazabilidad.

En 2025 se implementaron 20 reglas YARA para fortalecer la detección de amenazas en los asociados del sector financiero en Colombia. La mayor proporción se enfocó en ransomware y stealer con seis reglas cada uno, dadas sus implicaciones directas en la continuidad operativa y exposición de información sensible. El resto de las reglas complementa la cobertura frente a mecanismos de intrusión y control remoto como loader y RAT, además de amenazas específicas como Botnet y Keylogger. Esta distribución refleja una priorización basada en riesgo, alineada con las amenazas más relevantes para el contexto financiero del país y orientada a mejorar la capacidad de prevención y respuesta.

Identificación de familias mediante reglas YARA

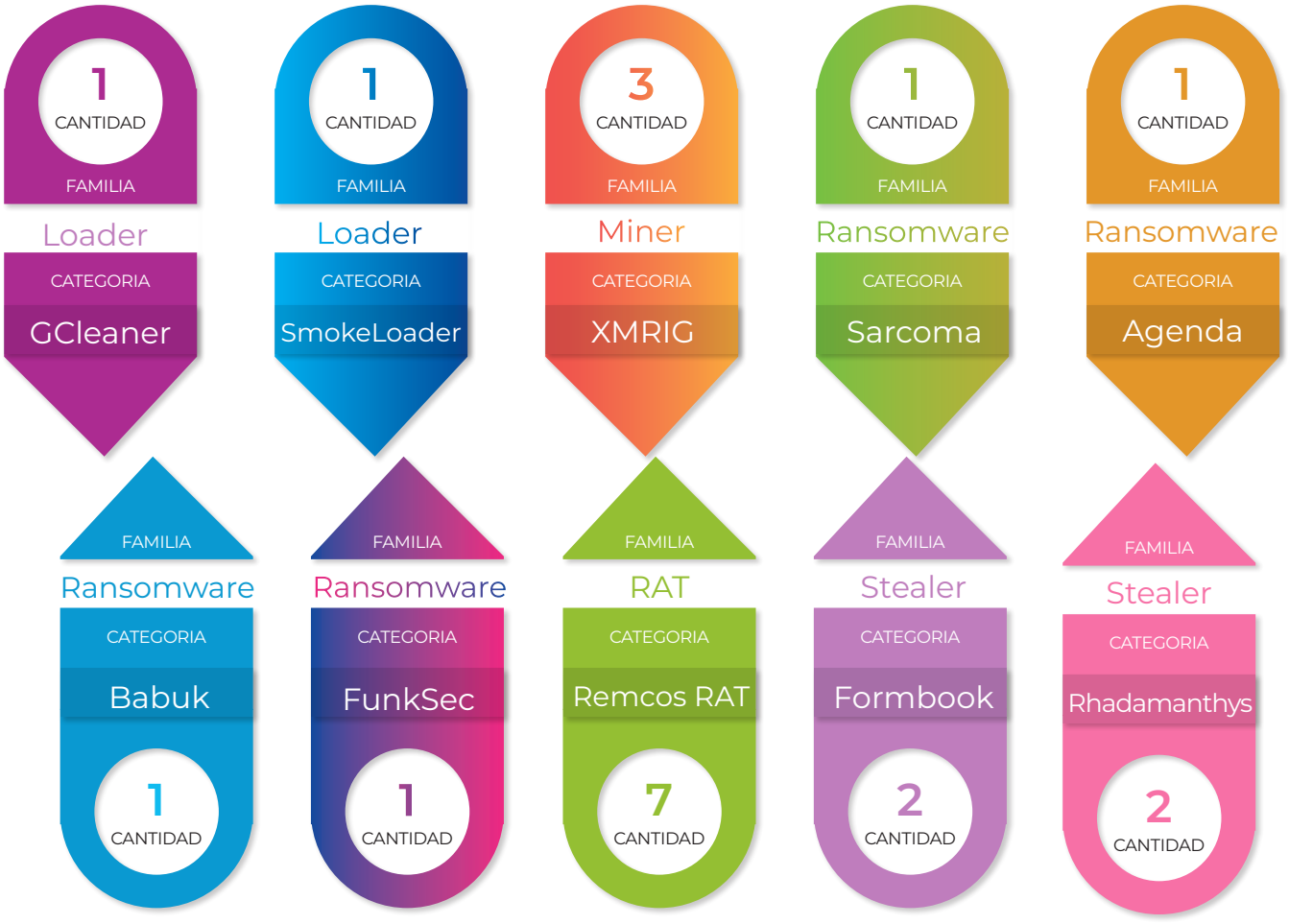
Gráfica 20. Identificación de familias mediante reglas YARA en 2025. Fuente: CSIRT Financiero.

Unified Threat Identification - SIGMA Rule

Una regla Sigma describe qué comportamiento sospechoso buscar y en qué tipo de registros (logsource), incorporando una lógica de detección basada en selecciones y una condición. Su principal ventaja es que estandariza la detección sobre logs y facilita su adopción en distintos entornos (normalmente en el contexto de un SIEM).

En 2025 se implementaron 28 reglas Sigma para asociados del sector financiero en Colombia, con el objetivo de fortalecer la detección temprana y la respuesta frente a amenazas relevantes para el sector. El esfuerzo se enfocó principalmente en RAT y malware tipo stealer, debido a su relación directa con accesos no autorizados, captura de credenciales y posibles escenarios de fraude. De manera complementaria, se incorporaron detecciones para troyanos bancarios, minería maliciosa, ransomware y mecanismos de carga inicial como loaders, además de herramientas utilizadas en distintas fases del ataque. En conjunto, esta cobertura amplía la visibilidad del ciclo de intrusión y contribuye a una postura de monitoreo más robusta para los asociados.

Identificación de familias mediante reglas SIGMA



Gráfica 21: Familias de malware identificado con reglas Sigma. CSIRT Financiero.

Endpoint Analysis

Es un análisis orientado a identificar técnicas maliciosas presentes en diferentes familias de malware, a partir del comportamiento observado en los endpoints. Esta investigación busca consolidar patrones de comportamiento que puedan repetirse en múltiples campañas, para convertirlos en capacidades de detección y mitigación aplicables según las tecnologías de defensa disponibles en cada asociado.

- Técnica MITRE ATT&CK T1574.001 (DLL Search Order Hijacking): hallazgo de alto riesgo que permite ejecutar código malicioso alterando el orden de búsqueda de DLL en Windows, abusando de aplicaciones legítimas. Esta técnica favorece la ejecución encubierta y la evasión de controles basados en firmas o hashes, con impacto potencial sobre la integridad del endpoint y la continuidad operativa.

- Técnica MITRE ATT&CK T1562 / T1562.001 (Impair Defenses – Disable or Modify Tools): comportamiento de riesgo crítico orientado a desactivar o alterar herramientas y controles de seguridad en Windows (p. ej., mediante PowerShell/CMD, cambios en registro y políticas). Reduce la visibilidad y capacidad de respuesta del endpoint, habilitando fases posteriores del ataque como movimiento lateral, captura de credenciales y fraude, especialmente relevante en el sector financiero.

Tras cada investigación realizada por el CSIRT Financiero se pone a disposición a través de Eaglesight a los asociados las reglas de seguridad para convertir el análisis de amenazas en controles aplicables a nivel de red. Su adopción es opcional y depende de la infraestructura y necesidades de cada asociado, facilitando la diseminación de inteligencia accionable sin imponer cambios.

Suricata

- De igual manera, los asociados que operan Suricata pueden generar reglas orientadas a la detección avanzada de amenazas, aprovechando los resultados de las investigaciones cuando este motor de inspección profunda forme parte de su infraestructura. Esta flexibilidad contribuye a una adopción eficiente de la inteligencia generada, maximizando su valor operativo sin afectar la autonomía técnica de cada asociado.

Network threat – Snort

- Para entornos que utilizan Snort, los asociados tienen la opción de generar reglas de detección basadas en los indicadores identificados durante las investigaciones. Estas reglas fortalecen la capacidad de monitoreo del tráfico de red y permiten mejorar la visibilidad sobre actividades sospechosas, siempre en función de la pertinencia y compatibilidad con sus plataformas de detección.

IPtables

- En el caso de IPtables, los asociados pueden optar por generar reglas orientadas al bloqueo y contención de comunicaciones maliciosas, si este mecanismo se ajusta a su entorno perimetral. Esta posibilidad permite aplicar controles preventivos de forma selectiva, alineados con las políticas internas y el diseño específico de cada infraestructura.

Threat Intelligence Exchange

La interconexión de instancias MISP transforma el intercambio de información en una defensa colectiva federada. Mediante este ecosistema, las entidades del sector financiero de Colombia y el CSIRT Financiero sincronizan inteligencia de amenazas en tiempo real. El objetivo no es solo compartir datos, sino correlacionar ataques y vulnerabilidades para generar una respuesta automatizada y proactiva, reduciendo drásticamente la exposición del sector ante amenazas dirigidas y sistémicas.

La importancia del intercambio de información para la inteligencia de amenazas se ve reflejada en:

- Detección temprana de amenazas: facilita la identificación proactiva de campañas maliciosas antes de que se materialicen en la infraestructura propia. Permite correlacionar y consumir TTP (Tácticas, Técnicas y Procedimientos) y artefactos maliciosos (IoC) en tiempo real, transformando la postura de seguridad de una detección reactiva a una alerta temprana basada en contexto.

- Mejora de la defensa: convierte la inteligencia compartida en reglas de defensa accionables. Al recibir telemetría detallada sobre vectores de ataque activos, las entidades pueden endurecer (hardening) sus controles de seguridad y desplegar contramedidas específicas de forma ágil, cerrando brechas de seguridad frente a tácticas emergentes antes de que puedan ser explotadas.

- Colaboración sectorial: reemplaza los silos de información estableciendo una red de confianza federada. El intercambio estructurado permite que las entidades financieras en Colombia dejen de defenderse de forma aislada y operen como un ecosistema unificado, capitalizando la experiencia colectiva para neutralizar amenazas transversales que apuntan al sector.

- Reducción de riesgos: minimiza la superficie de ataque y el impacto potencial de los incidentes. Al operar con visibilidad granular sobre el panorama de amenazas actual, la toma de decisiones evoluciona de la especulación a la gestión basada en evidencia, protegiendo proactivamente los activos críticos y blindando la reputación institucional frente a disrupciones.

Durante el periodo 2025, el CSIRT Financiero aseguró la interoperabilidad continua de la instancia MISP con 15 entidades del sector. Esta integración garantizó el flujo automatizado de Indicadores de Compromiso (IoC) en tiempo real, logrando una reducción tangible en la carga operativa de los equipos de seguridad y acelerando drásticamente los tiempos de triaje y respuesta ante incidentes en las entidades conectadas.

Gráfica 22. Entidades conectadas a Misp. Fuente: CSIRT Financiero.

Advanced Threat Emulation

Esta capacidad permite ejecutar escenarios de amenaza bajo condiciones controladas, emulando las Tácticas, Técnicas y Procedimientos (TTP) de adversarios y malware activos. Su objetivo es medir la efectividad real de la postura de seguridad de las entidades financieras, identificando brechas de detección y validando la resiliencia de la infraestructura frente a ataques dirigidos o transversales.

En 2025, el CSIRT Financiero realizó dos (2) emulaciones asociadas con tipos de malware presentes en campañas vistas en Colombia.

Emulación inyección de procesos

CRT-ATE-ME_2025-001: abril 2025

Emulación archivos SVG maliciosos

CRT-ME-2025-002: noviembre 2025

Threat Intelligence Prevention

Threat Intelligence Prevention es un servicio diseñado para identificar y analizar, de manera preventiva, ciberamenazas que afectan tanto al sector financiero colombiano como al panorama internacional, a través del uso de métricas y estadísticas clave que permiten anticipar riesgos potenciales y mitigar eventos o incidentes antes de que comprometan la confidencialidad, integridad y disponibilidad de la información en las organizaciones.

Con un enfoque basado en inteligencia de amenazas, el CSIRT Financiero ofrece una perspectiva estratégica que facilita a las entidades financieras la implementación de medidas proactivas y efectivas, adaptadas a un entorno digital en constante evolución.

Capacidades del servicio:

- Detectar y analizar patrones de amenazas emergentes mediante el uso de datos y estadísticas.
- Evaluar las tácticas, técnicas y procedimientos (TTP) habituales de los actores de amenaza para prever posibles ataques.
- Fortalecer las políticas internas de seguridad con información procesable basada en inteligencia.
- Promover la cooperación sectorial mediante el intercambio de información crítica para aumentar la resiliencia colectiva.
- Desarrollar estrategias preventivas que reduzcan la superficie de ataque y minimicen el impacto de acciones maliciosas.

Al aprovechar el potencial del análisis estadístico y las métricas generadas, Threat Intelligence Prevention permite a las entidades financieras estar un paso adelante, anticiparse a las amenazas y garantizar una respuesta eficaz frente a los riesgos cibernéticos.

Strategy CTI Office

Durante 2025, el CSIRT Financiero desempeñó un rol fundamental en la protección de la infraestructura cibernética de las entidades financieras en Colombia, impulsando la difusión de información estratégica sobre ciberamenazas a través del servicio Threat Intelligence Prevention y su subservicio Strategy CTI Office. Como parte de esta iniciativa, se compartieron boletines técnicos diseñados para proporcionar a las entidades financieras información relevante que les permite anticipar y mitigar riesgos de seguridad.

En este período, se distribuyeron doce (12) Security Bulletins con el objetivo de informar y concienciar sobre las amenazas más recientes y su impacto en el sector financiero, alertar sobre posibles riesgos y fortalecer las capacidades defensivas de las instituciones, promoviendo una postura proactiva frente a los ataques cibernéticos.

Asimismo, dentro del subservicio Strategy CTI Office, se compartieron cuatro (4) Strategy Bulletins, los cuales contienen análisis estratégicos sobre tendencias y amenazas que afectan al sector financiero en Colombia. Estos informes ofrecen una visión detallada del panorama de ciberseguridad cada tres meses, permitiendo a las entidades comprender la evolución de los riesgos y adoptar medidas preventivas más efectivas.

El CSIRT Financiero mantiene su compromiso con la difusión de información crítica y estratégica para fortalecer la resiliencia del sector ante amenazas emergentes. A través de esta labor, se promueve la colaboración y se refuerza la seguridad cibernética, garantizando un entorno más confiable para las entidades financieras del país.

Training hands-on (Webinars)

El CSIRT Financiero cuenta con tres espacios de entrenamiento, los cuales permiten el intercambio de experiencias y brindan nuevas herramientas para apoyar la adquisición de conocimientos en ciberseguridad, estos espacios son los siguientes:

- **CSIRT Training:** Espacio de sesiones de entrenamiento virtuales o presenciales hands -on, que fomentan el intercambio de mejores prácticas y proporcionando herramientas prácticas y metodologías.

- **CSIRT Experiences:** Encuentros virtuales para el intercambio de experiencias entre entidades financieras, expertos invitados y organizaciones externas. Su objetivo es analizar incidentes pasados y extraer lecciones valiosas que fortalezcan la resiliencia y la seguridad del sistema financiero.

- **CSIRT Cyber Webinar:** Sesiones virtuales sobre tendencias y actualizaciones en ciberseguridad con expertos internacionales. Proporcionan información y estrategias para fortalecer la seguridad en entidades financieras.

De acuerdo con lo anterior, el CSIRT Financiero realizó trece (13) Webinars que permitieron a los asociados entender y comprender, de forma estructurada, los riesgos y desafíos de la era digital. Asimismo, al compartir conocimientos y estrategias de protección, el CSIRT Financiero fortaleció la confianza de las entidades financieras demostrando su compromiso con la ciberseguridad.

CSIRT Financiero

· Red Nacional de SOC	(Mar 2025)
· Como atacan las amenazas avanzadas al entorno financiero por Telefónica	(Mar 2025)
· CSIRT Financiero - Webinar Tendencias 2025	(Mar 2025)
· Lanzamiento Memoria Anual 2024	(May 2025)
· Computación cuántica y ciberseguridad	(Jun 2025)
· Gestión y ciclo de vida de los IoC	(Jun 2025)
· Evaluando el ROI y ROA de la Ciberseguridad	(Jul 2025)
· Lanzamiento plataforma inteligencia de amenazas	(Jul 2025)
· CSIRT Financiero - Onboarding - Plataforma EagleSight	(Ago 2025)
· Workshop de capacidades y usos de la plataforma Eaglesight	(Ago 2025)
· Tendencias y criptografía en el sector financiero	(Oct 2025)
· Incidentes en terceros críticos	(Nov 2025)
· Ciber ejercicios en el Sector Financiero	(Nov 2025)

APT Monitor & Analysis Impact

Servicio de seguimiento y análisis de las principales APT a nivel global, enfocado en identificar a los actores, métodos de operación (modus operandi) y tácticas, técnicas y procedimientos (TTP). Este servicio permite a las entidades anticiparse a amenazas avanzadas, comprender patrones de ataque recurrentes y tomar decisiones informadas para fortalecer sus defensas. Además, proporciona inteligencia accionable que apoya la detección temprana, la mitigación de riesgos y la planificación de estrategias de ciberseguridad más efectivas frente a campañas sofisticadas y persistentes.

Estos son los actores que atacaron activamente infraestructuras en la región según reportes de inteligencia de 2025:

Actividad grupos APT en la región

Nombre Grupo APT	Acciones en 2025
APT-C-36 (Blind Eagle)	En 2025 mantuvo campañas masivas de spearphishing suplantando a la DIAN, Fiscalía y Juzgados. Utilizaron nuevas tácticas (archivos .url y explotación de CVE-2024-43451) para infectar instituciones gubernamentales y financieras en Bogotá y la región andina.
ShinyHunters	Responsables de la venta de datos masiva relacionada con la brecha de Snowflake (que afectó a millones de clientes en Chile, Uruguay y España). Su impacto en 2025 fue la monetización y extorsión secundaria de estos datos en foros clandestinos.
LockBit	LockBit regresó con su versión 5.0 en septiembre de 2025. Sigue siendo la franquicia de Ransomware-as-a-Service (RaaS) más activa en la región, afectando sectores de manufactura y servicios en Latam.

Hellcat	Un grupo de ransomware agresivo surgido a finales de 2024 y activo en 2025. Se les atribuyen ataques a grandes corporaciones de telecomunicaciones y energía.
Akira	Se consolidó en 2025 como una de las amenazas de ransomware dominantes en América Latina, llenando el vacío de grupos anteriores. Atacan indiscriminadamente a PyMES y entidades educativas.
Phantom Mantis	Campaña de ransomware dirigida a organizaciones latinoamericanas, explotando vulnerabilidades críticas en dispositivos Fortinet para ejecución remota y despliegue de cifrado, con impacto potencial extensivo en infraestructuras financieras y corporativas.
Red Akodon	Uso de AsyncRAT para captura de información y credenciales mediante phishing, dirigido a entidades financieras, gubernamentales y privadas en Colombia. (impacto directo en contexto nacional).
Nova (Ralord)	Ransomware RaaS comprometió 100 GB de datos sensibles de una entidad del estado, incluyendo procesos y correos institucionales. (impacto a la seguridad de datos e integridad sectorial).

Gráfica 23: Actividad grupos APT en la región. Fuente: CSIRT Financiero.

Relevant Event

Durante el 2025, el panorama de amenazas cibernéticas que impactó al sector financiero a nivel global se caracterizó por una sofisticación creciente de los actores maliciosos, la proliferación de campañas de ransomware de doble extorsión, el uso de ingeniería social y tácticas de evasión, así como la persistencia de APT con motivación financiera y geoestratégica. Muchos grupos tradicionales continuaron activos con nuevas variantes o técnicas, mientras emergieron actores con modelos Ransomware-as-a-Service (RaaS), intensificando tanto la escala como la eficiencia de sus ataques. Este año también mostró un aumento de campañas dirigidas que tuvieron impacto directo en infraestructuras críticas financieras y tecnológicas, lo que resalta la necesidad de un enfoque de defensa integral basado en inteligencia de amenazas, una estrategia de defensa en profundidad y respuesta coordinada a incidentes. En el análisis de eventos que sigue, se prioriza la relevancia de cada actividad destacada para el sector financiero a nivel global.

Eventos más relevantes 2025

1

Ciber espionaje de APT34 (OilRig/Helix Kitten) a entidades financieras y telecomunicaciones

Detalle: APT34, con historial desde 2014, ejecutó campaña persistente de espionaje centrada en sectores financiero y telecomunicaciones, utilizando malware personalizado y técnicas evasivas para extraer información crítica.

2

Actividad de Winnti/APT41 con RAT dirigidos a instituciones financieras

Detalle: Distribución de cargadores esteganográficas y RAT (GodRAT, AsyncRAT) enfocados en obtener control remoto, exfiltrar credenciales y explorar sistemas, afectando directamente objetivos financieros. (sin fuente web adicional para detalle específico de campaña).

3 **Operaciones de ransomware de Black Basta con exfiltración y evasión**

Detalle: Uso de phishing avanzado en Microsoft Teams y despliegue de múltiples herramientas para movimiento lateral, exfiltración de datos y cifrado prolongado en infraestructura crítica, demostrando tácticas robustas del modelo RaaS.

Detalle: Ransomware de doble extorsión activo desde 2025 con cifrado fuerte (Curve25519, ChaCha20), interrupción de servicios y destrucción de respaldos de una serie de víctimas afectando continuidad operativa de organizaciones.

Surgimiento e impacto rápido de DireWolf ransomware (doble extorsión) **4**

5 **Lazarus: campañas continuas y variantes orientadas a criptomonedas y sector financiero**

Detalle: Lazarus empleó técnicas como ClickFix, phishing con ofertas laborales falsas y variantes multietapa para comprometer sistemas Windows y macOS, exfiltrando datos y credenciales enfocadas en criptomonedas y activos financieros. (patrón persistente con múltiples fases).

Detalle: APT financiera que empleó rootkit CAKETAP y dispositivo físico Raspberry Pi para manipular mensajes HSM de cajeros automáticos, facilitando retiros no autorizados y elusión de detección tradicional. (alto impacto operacional y fraude financiero).

UNC2891 — intrusión avanzada en infraestructura bancaria y redes de cajeros automáticos **6**

Gráfica 24. Eventos Relevantes 2025. CSIRT Financiero.

Tendencias en ciberseguridad 2026

En 2026, se perfila como un periodo de profundos cambios marcados por la acelerada digitalización de los servicios financieros y avances tecnológicos exponenciales que amplían de forma significativa la superficie de ataque.

Ante este escenario, la ciberseguridad deja de ser un complemento para convertirse en el eje sobre el que debe articularse la estrategia empresarial.

Las organizaciones disponen de un margen de maniobra cada vez más limitado para adaptarse a las nuevas reglas de la transformación digital, los riesgos emergentes y las expectativas de resiliencia, confianza y continuidad operativa, en un entorno cada vez más interconectado.

Comprender las proyecciones y dinámicas 2026 es clave para que las instituciones financieras identifiquen riesgos, anticipen desafíos y guíen sus decisiones estratégicas.

Tendencias en el sector financiero

Troyanos por WhatsApp

En 2025 y comienzos de 2026, se ha detectado un aumento de campañas que emplean la aplicación de mensajería instantánea WhatsApp como vector de distribución de malware bancario. Los atacantes se aprovechan de la amplia base de usuarios de esta aplicación y la confianza entre los contactos para ampliar su tasa de propagación y, con ello, las probabilidades de éxito.

En lugar de recurrir al correo electrónico tradicional, los ciberdelincuentes optan por enviar archivos maliciosos a través de WhatsApp. Al ser ejecutados, estos archivos pueden comprometer sistemas infectados y extraer credenciales financieras mediante sofisticados mecanismos de auto propagación a través de la lista de contactos de la víctima.

Esta técnica ha sido utilizada extensamente en Brasil, con amenazas como Astaroth. No obstante, en la región se ha detectado la presencia de un modelo más moderno

y sofisticado, conocido como Maverick, que emplea la IA generativa para adaptar sus ataques y mejorar sus técnicas de propagación y evasión.

El proceso de infección comienza cuando el destinatario recibe un mensaje acompañado de un archivo ZIP con apariencia legítima, que simula ser un recibo, una factura o un documento bancario. En su interior se aloja un fichero LNK malicioso de Windows.

Al ejecutarse, este archivo inicia una compleja cadena de infección orientada a tomar el control completo del dispositivo. El programa verifica que el sistema de la víctima esté ubicado en Brasil y, posteriormente, monitoriza su actividad en diversidad de plataformas bancarias. Cuando el usuario accede a su entidad financiera, el troyano lo detecta y descifra un módulo que se ejecuta en segundo plano, habilitando capacidades como la extracción de credenciales, registro de pulsaciones de teclas, lanzamiento de páginas de phishing superpuestas y manipulación de procesos.

Esta amenaza representa el futuro del fraude bancario, ya que su arquitectura modular, junto con su alto nivel de eficacia y sofisticación le confieren un notable potencial para replicarse en otras regiones del mundo.

Código QR malicioso

América Latina experimentó durante 2025 uno de los crecimientos más rápidos en el uso de códigos QR como método de pago, superando incluso a Europa en términos de adopción general de esta tecnología.

En Colombia, las transacciones efectuadas mediante códigos QR aumentaron en 2024 un 85%[1], cifra que reflejan su acelerada integración en los hábitos de comercios y consumidores de todo el país.

La incorporación de esta nueva tecnología en el ecosistema de pagos ha captado la atención de los actores criminales. La modalidad de ataque basada en código QR se conoce como quishing, un término que procede de la combinación de QR + phishing, y que consiste en la utilización de estos elementos como vector principal de engaño.

[1] *https://www.valoraanalitik.com/pagos-con-codigos-qr-se-disparan-en-colombia-mas-de-300-millones-de-transacciones-en-2024/*

En este tipo de campañas, los atacantes distribuyen etiquetas con códigos QR que, al ser escaneadas por el destinatario, redirigen a un sitio web fraudulento o desencadenan la descarga de malware.

Esta variante de phishing reviste una peligrosidad particular debido a la ausencia de indicadores visuales que posibiliten su detección. A diferencia de los enlaces habituales, en los que resulta más sencillo identificar caracteres erróneos o patrones anómalos, el usuario accede directamente al destino final tras el escaneo.

Además, los sistemas de seguridad de dispositivos móviles o del correo electrónico no suelen detectar los enlaces maliciosos en los archivos con formato de imagen.

A esto se añade el contexto de confianza en el que suelen emplearse los códigos QR, como en comercios, restaurantes y bancos, lo que reduce el nivel de sospecha para los usuarios.

Varios informes recientes señalan que este tipo de ataques han aumentado hasta cinco veces a finales del año 2025, con múltiples campañas de correo electrónico que utilizan QR para ocultar enlaces maliciosos.

De cara a 2026, estos códigos evolucionarán en apariencia y estructura. Se combinarán tácticas más sofisticadas, como textos y señuelos generados con Inteligencia artificial (IA) para reforzar su apariencia y credibilidad y agravar las dificultades de detección, tanto por los usuarios como por los mecanismos de seguridad tradicionales.

Zero-Trust 2.0

La premisa de no confiar implícitamente en nada dentro ni fuera de la red se ha convertido en la base de las estrategias de ciberseguridad modernas, especialmente en sectores críticos como el financiero. La protección de datos sensibles y la prevención de fraudes requieren controles exhaustivos y verificaciones continuas de usuarios, dispositivos y transacciones.

Aunque el modelo Zero Trust comenzó a implementarse hace más de una década, la pandemia aceleró significativamente su adopción, consolidándose como una necesidad operativa y no como una mejor práctica.

"El auge del código QR malicioso consolida a Zero Trust 2.0 como pilar clave en la prevención del fraude digital."

Según diversos estudios, se prevé que el mercado de Zero Trust crecerá de forma sostenida en Latinoamérica, con un aumento promedio anual del 17% hasta el 2030[2]. Estas proyecciones revelan la inversión real y confirman que Zero Trust ha dejado de ser una aspiración para convertirse en un estándar de seguridad.

La proliferación de amenazas cada vez más sofisticadas, requiere una arquitectura de seguridad más adaptativa y evolucionar hacia un modelo más dinámico. El modelo Zero Trust se ha extendido más allá de la red tradicional, trasladando el límite de seguridad hacia la identidad y el contexto de cada acceso.

Aunque los principios sobre los que se rige Zero Trust no han cambiado, sí lo ha hecho la forma en como se aplican.

Las organizaciones ya no operan en entornos claramente definidos y delimitados. La adopción de infraestructura en la nube, el trabajo remoto y las plataformas SaaS (Software as a Service) han diluido el perímetro tradicional, haciendo obsoleto el modelo de seguridad basado exclusivamente en la protección del acceso externo.

Esta nueva generación, denominada popularmente como Zero Trust 2.0, representa una evolución clave para el sector financiero, al integrar nuevas capas de seguridad y capacidades avanzadas, como la inteligencia contextual y el análisis comportamental, que permiten la adopción de respuestas dinámicas y en tiempo real.

En un escenario marcado por la digitalización de los servicios financieros, el aumento de los incidentes de ciberseguridad y de los accesos desde diversos canales, este modelo de seguridad permite evaluar de manera continua elementos como la identidad del usuario, el estado del dispositivo o el tipo de transacción.

Los mecanismos de control se adaptan al nivel de riesgo, reforzando la protección de datos sensibles y operaciones críticas, sin alterar la experiencia del usuario.

[2] *https://www.grandviewresearch.com/horizon/outlook/zero-trust-security-market/latin-america*

Ataques dirigidos a pagos NFC

En 2026 también se prevé un incremento de campañas dirigidas a las transacciones de pago sin contacto (NFC), impulsado por la adopción masiva de este método tanto en tarjetas físicas como en wallets.

Los criminales están desarrollando herramientas diseñadas para explotar las vulnerabilidades relacionadas con este sistema de pago.

"La evolución de ataques a pagos NFC redefine la seguridad en entornos de proximidad."

Aunque el método de pago por proximidad incorpora mecanismos de seguridad avanzados, como el token digital único y cifrado para cada transacción, ya se han detectado nuevos esquemas de fraude capaces de eludir estos controles mediante ataques que combinan tecnologías y manipulación de los usuarios.

Este tipo de fraude presenta dos modalidades principales, una presencial y otra remota.

La primera se basa en la proximidad física y se aprovecha de la rapidez del NFC para actuar de manera desapercibida. Los atacantes utilizan dos dispositivos móviles: uno de ellos será el que se sitúa cerca del dispositivo de la víctima para robar el token de pago generado durante la transacción. Este código será enviado en tiempo real al segundo dispositivo, desde el que se procesa una transacción fraudulenta en un terminal de pago legítimo. En la mayoría de los casos, la víctima no se percata inmediatamente de ese pago.

Con respecto a la modalidad en remoto, comienza con ingeniería social. El atacante contacta con la víctima, actuando en representación de una entidad financiera u organismo y le persuade para que descargue una aplicación maliciosa y, a continuación, valide su tarjeta bancaria. Durante este proceso, la aplicación intercepta el token generado por el sistema de pago y lo reutiliza para autorizar transacciones fraudulentas desde otro dispositivo o entorno controlado por el atacante.

Este tipo de fraude muestra cómo los atacantes se adaptan a los nuevos hábitos de consumo digital; combinan técnicas tradicionales de engaño con tecnologías emergentes y perfeccionan sus herramientas para tratar no solo las debilidades del protocolo NFC, sino el contexto de su uso, los dispositivos y el factor humano.

"Una amenaza transversal en un perímetro que ya no existe".

Tendencias en el sector tecnológico

Inteligencia artificial: una amenaza transversal

La inteligencia artificial se ha consolidado durante 2025 como un componente fundamental dentro de la ciberseguridad, y el nuevo año augura una tendencia similar en este ámbito.

Aunque la perspectiva humana en la ciberseguridad es indispensable, la implementación de inteligencia artificial supone la liberación de los analistas para dedicarse a tareas más estratégicas mediante la automatización de los procesos rutinarios. Esto también trae consigo otros beneficios, como la reducción del error humano en procesos delicados y la mejoría en la toma de decisiones, al identificar y corregir posibles deficiencias en la estrategia de seguridad.

No obstante, los beneficios de la utilización de la inteligencia artificial no han pasado desapercibidos para los ciberdelincuentes. Esta poderosa herramienta abre un nuevo paradigma en la realización de ataques más especializados y dañinos. No solo supone una actualización para los ataques más clásicos, como las suplantaciones de identidad en tiempo real mediante deepfakes, sino la creación de nuevos ataques y superficies de ataque. Un ejemplo de esto lo vemos en el troyano Maverick, ya citado anteriormente, descubierto a finales de 2025, que utiliza la inteligencia artificial Generativa para reescribir su propio código en tiempo real, evadiendo así los principales sistemas de seguridad que basan sus detecciones en firmas concretas.

No hay duda de que la IA ha supuesto un antes y un después en el mundo de la ciberseguridad, tanto para las compañías e instituciones como para los actores maliciosos, por lo que debemos estar pendientes de las nuevas posibilidades que ofrecerá esta herramienta durante 2026

Edge computing: el nuevo perímetro

Sin duda, el Edge computing será una de las principales tecnologías de 2026.

La distribución de capacidades de procesamiento que ofrece esta tecnología, que se acerca a los dispositivos mediante nodos edge, y permite reducir la latencia en la toma de decisiones de la inteligencia artificial, además, mejora la privacidad de

los datos que procesan al transportar a la nube solo los datos esenciales.

En la actualidad, el número de IoT conectados supera los 15.000 millones de dispositivos, y se estima que en la próxima década la cifra se duplique[3], lo que implica la existencia de una necesidad real de procesar los datos cerca del origen para reducir la latencia en cuestiones esenciales.

Este tipo de procesamiento amplía notablemente los horizontes de la IA, permitiendo una usabilidad en dispositivos prácticamente autónomos que solo hacen uso de los servidores para los procesos más complejos.

Además, la mejora de la privacidad que ofrece el edge computing constituye una optimización del uso corporativo de la IA. A este respecto, aunque no se dispone de una cifra oficial, Intel estimaba que durante 2025 más del 50% de los datos empresariales estarían fuera de la nube ; por otro lado, Gartner estimó esta cifra en un 75% .

El desafío cuántico

La computación cuántica es la gran promesa de la década. Esta tecnología se proyecta como una revolución real y tangible con impacto en múltiples ámbitos.

Uno de los campos que revolucionará es, sin duda, la seguridad de los datos, prometiendo desfasar los principales sistemas de cifrado de clave pública actuales.

Aunque la computación cuántica no ha alcanzado todavía este objetivo, algunas organizaciones multilaterales como la UE y algunos países como Estados Unidos han comenzado a desarrollar sistemas de cifrado postcuánticos para securitizar la información tras la tecnología cuántica.

A este respecto, los esfuerzos públicos principales son notables, por ejemplo, el NIST lidera el esfuerzo nacional estadounidense para asegurar la información electrónica ante la amenaza futura que representa la capacidad de procesamiento postcuántico, recibió 69 algoritmos candidatos en la primera fase de estandarización PQC y seleccionó 4 algoritmos finales en 2024.

"El desafío cuántico: la próxima revolución tecnológica que pondrá en riesgo los modelos actuales de cifrado y obligará a redefinir la seguridad de la información".

[3] *https://www.interempresas.net/TIC/566053-El-futuro-del-IoT-pasa-por-una-migracion-planificada-del-parque-de-dispositivos-2G-y-3G.html*

Por otro lado, la Unión Europea ha establecido 2030 como horizonte para que las infraestructuras críticas estén preparadas para la transición poscuántica.

Riesgos en la cadena de suministro

Los ataques a la cadena de suministro de software se han consolidado como una de las amenazas más críticas y de más rápido crecimiento en el panorama de la ciberseguridad. Estos ataques explotan la relación de confianza entre entidades, comprometiendo proveedores, paquetes de software de código abierto y otros componentes de terceros para infiltrarse indirectamente en sus objetivos finales.

"La cadena de suministro se ha convertido en el nuevo vector crítico de ataque, donde la confianza entre terceros es explotada para comprometer a gran escala.".

En septiembre de 2025, un ataque de phishing dirigido a un desarrollador del registro de paquetes de Node.js (NPM) condujo al compromiso de 18 paquetes de software, que en conjunto suman más de 2,6 mil millones de descargas semanales. El código malicioso inyectado fue diseñado para secuestrar transacciones de criptomonedas directamente desde los navegadores de los usuarios. Poco después, en octubre de 2025, el grupo de ciberdelincuentes Crimson Collective se atribuyó el robo de aproximadamente 570 GB de datos de una instancia de GitLab de Red Hat Consulting, exponiendo informes de clientes como Bank of America, T-Mobile y agencias gubernamentales de EE. UU.

Estos eventos muestran que los sistemas de seguridad perimetral tradicionales son insuficientes. Para contrarrestar la amenaza que suponen los ataques a la cadena de suministro, las organizaciones deben adoptar un enfoque de confianza cero (Zero Trust) con todas las partes implicadas en el proceso productivo, además de evaluar continuamente la postura de seguridad de los proveedores.

[4]https://www.datacentermarket.es/datacenter-infrastructure/el-50-de-los-datos-empresariales-estaran-fuera-de-los-data-centers-y-la-nube-en-2025/?utm_source=copilot.com
[5]https://www.sydle.com/es/blog/edge-computing-6255a8bb3bbdd676573d5af3

ASOBANCARIA

Jonathan Malagón González

Presidente

Mónica María Gómez Villafañe

Vicepresidente Administrativa y Financiera

Angela María Vaca Bernal

Directora Dirección de Programas de Innovación Gremial

Sergio Andrés Silva Perico

Líder Dirección de Programas de Innovación Gremial

Gineth Stephany Colmenares Ortiz

Profesional Dirección de Programas de Innovación Gremial

CSIRT Financiero (MNEMO)

Carlos Javier Beltrán Camacho

Director de Operaciones

Belén Viqueira Sierra

Jorge Andrés Chaves Martínez

Paula Natalia Orjuela Calderón

Lady Zolanyi Páez Cortés

Oscar Fabián Quiroga Lozano

Juan David López Zamora

Camilo Ramírez Alarcón

Mario Zamarro Atilano

Carlos García Gálvez

Sonia González Escarda

ALCG DISEÑO • PUBLICIDAD

Adriana Lucía Cuéllar González

Diseño y Diagramación

CSIRT FINANCIERO

Aso Ban Caria

www.csirtasobancaria.com
csirt@asobancaria.com
incidente@csirtasobancaria.com
Cel.: +57 3174345665