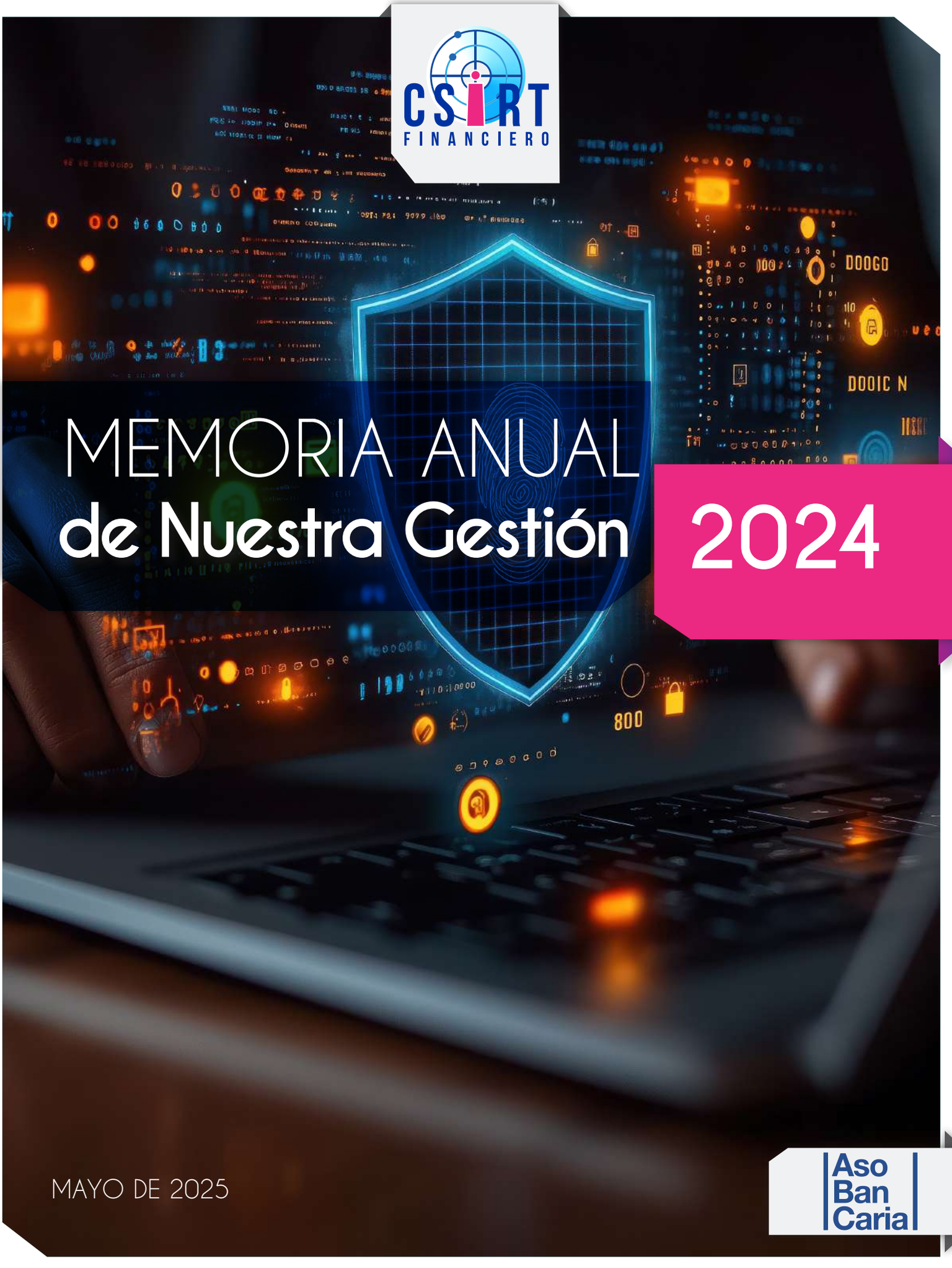



# MEMORIA ANUAL de Nuestra Gestión 2024

MAYO DE 2025

Aso Ban Caria

# ÍNDICE

# 1. Prólogo

**Por: Banco de la República de Colombia**

Ya dejó de sorprender el hecho de encontrar cada año mayores desafíos en el campo de la ciberseguridad para todos los sectores a nivel global. En un mundo cada vez más digitalizado e interconectado, la protección cibernética se ha convertido en un pilar fundamental para la estabilidad y confianza en las operaciones, especialmente del sector financiero. En este contexto, durante 2024 creció el número de ataques, su efectividad y complejidad; siendo de particular relevancia los de tipo ransomware por su alto impacto. Las principales causas de estos ataques identificados para el mismo periodo corresponden a explotación de vulnerabilidades (registrándose un incremento del 39% respecto a 2023 [1]), credenciales comprometidas y correos maliciosos [2]. Así mismo, la fuga de información [3] y los ataques a la cadena de suministro estuvieron presentes, teniendo estos últimos gran presencia mediática dado su impacto en la disponibilidad de servicios a nivel global [4]. Para enfrentar estos desafíos durante el año pasado, seguramente el trabajo de muchos se enfocó en adoptar buenas prácticas, fortalecer defensas cibernéticas y promover una cultura de higiene digital al interior de las entidades y en las interacciones con clientes y aliados que permitieran mitigar o anticiparse a esos riesgos materializados en otras empresas de todas las verticales.

En el ámbito de las buenas prácticas, la adopción de marcos de referencia como el NIST-CSF o la norma ISO 27001, o la aplicación a certificaciones tipo PCI o SWIFT CSP, han sido fundamentales para el ecosistema financiero. Estos estándares permiten identificar y priorizar iniciativas de mejora continua en la madurez de la gestión de riesgos de ciberseguridad. Al seguir estas directrices, las entidades financieras han podido fortalecer sus sistemas de gestión de seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de sus activos digitales mientras se promueve un entorno digital más seguro y resiliente. Aunque la adopción de estos marcos no es una "bala de plata", sí contribuye a la identificación y priorización de oportunidades para fortalecer la postura de seguridad de las entidades, demostrando un compromiso con la protección de la información y la resiliencia operativa.

*En este contexto, durante 2024 creció el número de ataques, su efectividad y complejidad; siendo de particular relevancia los de tipo ransomware por su alto impacto.*

Mirando hacia el futuro, ¿cómo seguir fortaleciendo los esquemas de ciberdefensa en este 2025? Un primer paso es reforzando los espacios de colaboración, tanto físicos como tecnológicos, con entidades nacionales e internacionales para que ese esfuerzo conjunto ayude a enfrentar las amenazas emergentes y proteger la integridad de sistemas y datos. Es por esto por lo que compartir y consumir inteligencia de amenazas en las operaciones de seguridad sigue jugando un papel crucial como una estrategia tecnológica proactiva para lograr detección temprana de amenazas y para implementar ejercicios de cacería en los ambientes corporativos. Este intercambio de información contribuye a la creación de un entorno financiero más seguro a nivel local y global.

Por otra parte, dado que dos de los vectores de ataque más exitosos continúan siendo el robo de credenciales y el envío de correos maliciosos, es imperativo seguir promoviendo una cultura de higiene digital, entendida como la implementación de políticas y procedimientos que aseguren el uso seguro y responsable de los recursos tecnológicos en las organizaciones.

Durante 2025, es importante seguir trabajando y fortaleciendo las capacidades de ciberdefensa pues, según el informe del Foro Económico Mundial (WEF) sobre riesgos globales [5], la ciberseguridad sigue siendo una de las principales preocupaciones a nivel mundial. Se estima que el sector financiero seguirá enfrentando un aumento de los ataques de ransomware con el agravante de la extorsión multifacética [6] definida por Mandiant como la utilización de múltiples puntos de ataque, incluyendo el cifrado de datos, el robo de estos y el señalar y avergonzar públicamente a la organización víctima [7]. Adicionalmente, como los ciberdelincuentes están usando la IA y el ML para sofisticar, automatizar y personalizar ataques haciéndolos más difíciles de detectar y prevenir, se requiere mantener una vigilancia constante y fortalecer la capacidad de adaptación continua a las amenazas en evolución.

Los ciber-riesgos, potenciados por el uso de IA para instrumentarlos, siempre estarán presentes en el sector financiero. Sin embargo, a favor de la ciberdefensa, estas mismas tecnologías emergentes también pueden ser una poderosa herramienta ya que la inteligencia artificial y el aprendizaje automático permiten detectar amenazas en tiempo real, optimizar la etapa de triage, automatizar las respuestas, disminuir los falsos positivos, entre otros, mejorando la eficiencia y precisión en las operaciones de defensa. Entonces, al entender el impacto y acoger estas tecnologías en las estrategias de seguridad digital se puede fortalecer la resiliencia del sector financiero y mejorar la protección de los activos digitales.

Finalmente, ante los retos que depara este año y los futuros, el éxito vendrá de la mano del trabajo en equipo a la vez que se promueve la cultura de higiene digital y la adopción de las mejores prácticas en ciberseguridad. De forma conjunta, con creatividad, proactividad y colaboración, será más fácil superar los desafíos que se presentan en el camino.

***[1]*** *2024 Cybersecurity Vulnerability Stats & Trends | SecurityVulnerability.io*

***[2]*** *https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf*

***[3]*** *https://www.welivesecurity.com/es/cibercrimen/incidentes-ciberseguridad-2024-america-latina/*

***[4]*** *https://securelist.lat/ksb-story-of-the-year-2024/99459/*

***[5]*** *https://www.weforum.org/publications/global-risks-report-2025/*

***[6]*** *https://cloud.google.com/security/resources/cybersecurity-forecast*

***[7]*** *https://www.mandiant.com/sites/default/files/2022-03/multifaced-extortion-eb-00396-02-es-LA.pdf*

# 2. Resumen ejecutivo

Estimados asociados, nos complace presentar el consolidado de las actividades llevadas a cabo por el CSIRT Financiero durante la vigencia 2024. Nuestro compromiso continuo con la protección de la información y la seguridad de los sistemas financieros ha sido una prioridad fundamental a lo largo de este año.

Ha sido un periodo desafiante y de transformación para el sector financiero colombiano y en el que el CSIRT Financiero desempeñó un papel crucial en la prevención, detección y respuesta a incidentes de ciberseguridad, fortaleciendo la resiliencia del ecosistema financiero ante amenazas cada vez más sofisticadas.

Se logró un aumento en la capacidad de detección temprana gracias a la implementación de nuevas tecnologías de inteligencia de amenazas y análisis de comportamiento.

Se gestionaron más de 500 eventos de seguridad, destacando un incremento en ataques de troyanos de acceso remoto (RAT), en comparación con 2023, con respuestas oportunas que minimizaron el impacto.

Se emitieron alertas tempranas sobre vulnerabilidades críticas y campañas de ciberataques emergentes, contribuyendo a la prevención proactiva de riesgos.

Reafirmamos nuestro compromiso con la seguridad del sector financiero, avanzando hacia un ecosistema más resiliente y preparado para enfrentar los desafíos cibernéticos del futuro. Los logros alcanzados en 2024 sientan bases sólidas para continuar protegiendo la integridad, confidencialidad y disponibilidad de la información financiera del país.

Gracias a los miembros del CSIRT Financiero por sus aportes de información, su compromiso de colaboración, intercambio de conocimiento y experiencia para hacer más seguro el ecosistema financiero. Seguimos comprometidos con la mejora continua y la adaptación frente a un entorno de amenazas en constante evolución.

Atentamente,

**Equipo del CSIRT Financiero**

# 3. Resumen Servicios CSIRT Financiero

Comprometido con la mejora continua, el CSIRT Financiero llevó a cabo diversas investigaciones sobre ciberamenazas que, de forma directa o transversal, pudieron llegar a impactar 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.

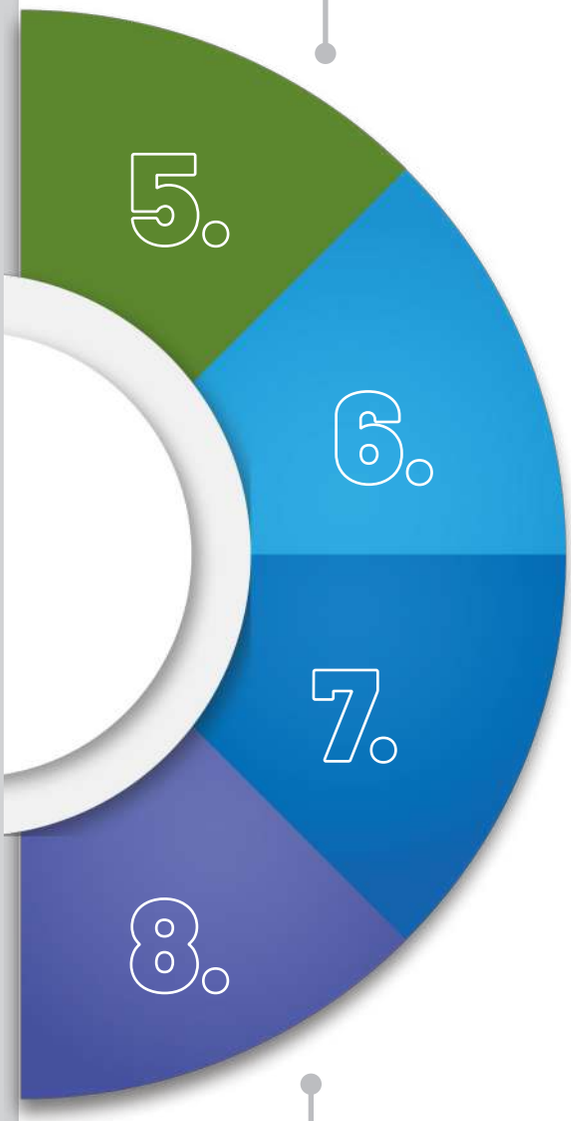
**Threat Intelligence Prevention:** Enfocado en la identificación y análisis proactivo de amenazas dirigidas al sector financiero, se compartieron (26) productos que permitieron a las entidades tomar decisiones estratégicas frente a diversas ciberamenazas que impactaron la industria.


**Strategy CTI Office:** A través de un análisis sobre información consolidada de forma mensual y trimestral, se identifican tendencias clave y evolución de amenazas. En este período, se compartieron (16) productos con el propósito de ofrecer una visión detallada del panorama de ciberamenazas que afectaron directa o indirectamente al sector financiero en Colombia.

**APT Monitor & Analysis Impact:** Fruto del seguimiento y análisis de las principales amenazas persistentes avanzadas (APT), incluyendo sus actores, modus operandi y técnicas, se elaboraron nueve (9) productos enfocados en estos grupos de amenazas que comprometen la infraestructura tecnológica en Colombia.

**Threat Intelligence Response:** Proporciona inteligencia de amenazas y análisis de riesgos para fortalecer la respuesta y la remediación tanto estratégica como operativa; a través de este servicio, se compartieron más de 1.200 productos, lo que permitió identificar cadenas de infección utilizadas por actores maliciosos y sus familias de malware. El CSIRT Financiero enfatiza la importancia de reconocer y mitigar las tácticas y técnicas empleadas por los atacantes, para reforzar las herramientas de seguridad perimetral y reducir el impacto de actividades maliciosas.

**Threat Analysis & Modeling:** Analiza eventos de seguridad, actores de amenazas, malware, arquitecturas y vulnerabilidades. En este ámbito, el CSIRT Financiero compartió 629 productos, permitiendo la identificación de patrones y comportamientos de amenazas dirigidas contra la infraestructura tecnológica de sus asociados.




**Advanced Threat Emulation:** Simula las actividades de los actores de amenazas mediante la ejecución controlada de malware. En este contexto, se entregaron dos (2) productos que facilitaron la replicación del comportamiento de las amenazas y generación de reglas de detección para herramientas de seguridad perimetral, con el objetivo de fortalecer las capacidades de detección y mitigación dentro de las organizaciones.

**Threat Security Response:** Gestiona el conocimiento, los procesos y las acciones necesarias para una respuesta efectiva ante eventos o incidentes de seguridad. En este marco, se desarrollaron tres (3) productos, incluyendo 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 534 reportes relacionados con phishing, distribución de malware, suplantación de aplicaciones y abuso de marca.

**Threat Detections & Prevent:** Genera inteligencia de amenazas aplicables en infraestructuras de seguridad y equipos de Blue Team. Con el propósito de mitigar tácticas y técnicas maliciosas, el CSIRT Financiero compartió 44 productos, incluyendo reglas YARA y SIGMA, fortaleciendo así las capacidades de defensa adaptativa ante amenazas dirigidas al sector financiero en Colombia.

# 4. Resumen entregables CSIRT Financiero

A través de nuestros servicios se compartieron más de 1.230 productos y más de 65.000 indicadores de compromiso, gracias a las diversas investigaciones de las diferentes ciberamenazas que afectan al sector financiero en Colombia.

| | | | |
|---|---|---|---|
| Security Bulletin (SB): | 12 | Monitoring Threat Analysis (MTA): | 1 |
| Strategy Bulletin (STRB): | 4 | Threat Focus Report (TFR) / Monographics: | 9 |
| Memoria Anual (MEA): | 1 | Malware Emulation (ME): | 2 |
| Relevant Events (RE): | 9 | Threat Uses Cases (TUC): | 1 |
| Cyber Security Warning (CSW): | 513 | Incident Response Playbook (IRP): | 2 |
| Tailored Threat Analysis - AGL: | 22 | Support Incident Response (SIR): | 534 |
| Tailored Threat Analysis - ASL: | 6 | Malware Activity - YARA (MA): | 21 |
| Tailored Threat Analysis - IOC: | 7 | Unified Threat Identification - Sigma (UTI): | 23 |
| Tailored Threat Analysis - TMP: | 37 | Webinar: | 9 |
| Vulnerability Threat Monitoring (VTM): | 34 | Indicadores de Compromiso: | 65.267 |

***Gráfico 1.*** *Resumen entregables Csirt Financiero. Fuente: CSIRT Financiero.*

# 5. Panorama global de ciberamenazas en Colombia 2024

El año 2024 fue un periodo crítico para la ciberseguridad en Colombia. Durante este tiempo, el país experimentó un incremento significativo en los ataques cibernéticos, con una sofisticación creciente de las amenazas y una afectación directa a sectores clave como el financiero, gubernamental y de infraestructuras críticas.

Los ataques de ransomware fueron una de las mayores amenazas en 2024. Grupos como LockBit, BlackCat (ALPHV) y CIOp centraron sus esfuerzos en entidades gubernamentales y financieras.

Dentro de las técnicas más utilizadas por estos grupos se destacan las siguientes:

- Uso de exploits de día cero para acceder a redes.
- Movimientos laterales en infraestructuras TI antes de la ejecución del cifrado.
- Doble extorsión con exfiltración de datos.

Las campañas de concienciación y el refuerzo de medidas de seguridad no fueron suficientes para frenar la tendencia, lo que evidenció la necesidad de estrategias más robustas en protección de datos.

El phishing continuó siendo una de las amenazas más prevalentes en Colombia. Durante 2024, los ciberdelincuentes perfeccionaron sus técnicas mediante el uso de inteligencia artificial y deepfakes para suplantar identidades de empresas y funcionarios gubernamentales.

Con relación a esto, se observaron las siguientes tendencias:

- Incremento de phishing bancario, con ataques que simulaban ser entidades financieras reconocidas.
- Uso de inteligencia artificial para generar correos más convincentes.
- Expansión del vishing (phishing por voz) y smishing (phishing por SMS) para engañar a los usuarios.

En respuesta, muchas organizaciones adoptaron autenticación multifactor (MFA) y sistemas de detección avanzada, aunque, en algunos casos, los atacantes lograron evadir estas medidas.

En 2024, el sector financiero enfrentó amenazas cada vez más sofisticadas, incluyendo troyanos bancarios, troyanos de acceso remoto (RAT) y ataques a sistemas de pago. Por el contrario, el sector energético, de telecomunicaciones y salud fueron objetivos clave de grupos APT (Amenazas Persistentes Avanzadas) como APT29 (Cozy Bear) y APT41. Todo esto evidencia la necesidad de regulaciones más estrictas y una cooperación internacional más efectiva en la defensa de las infraestructuras críticas.

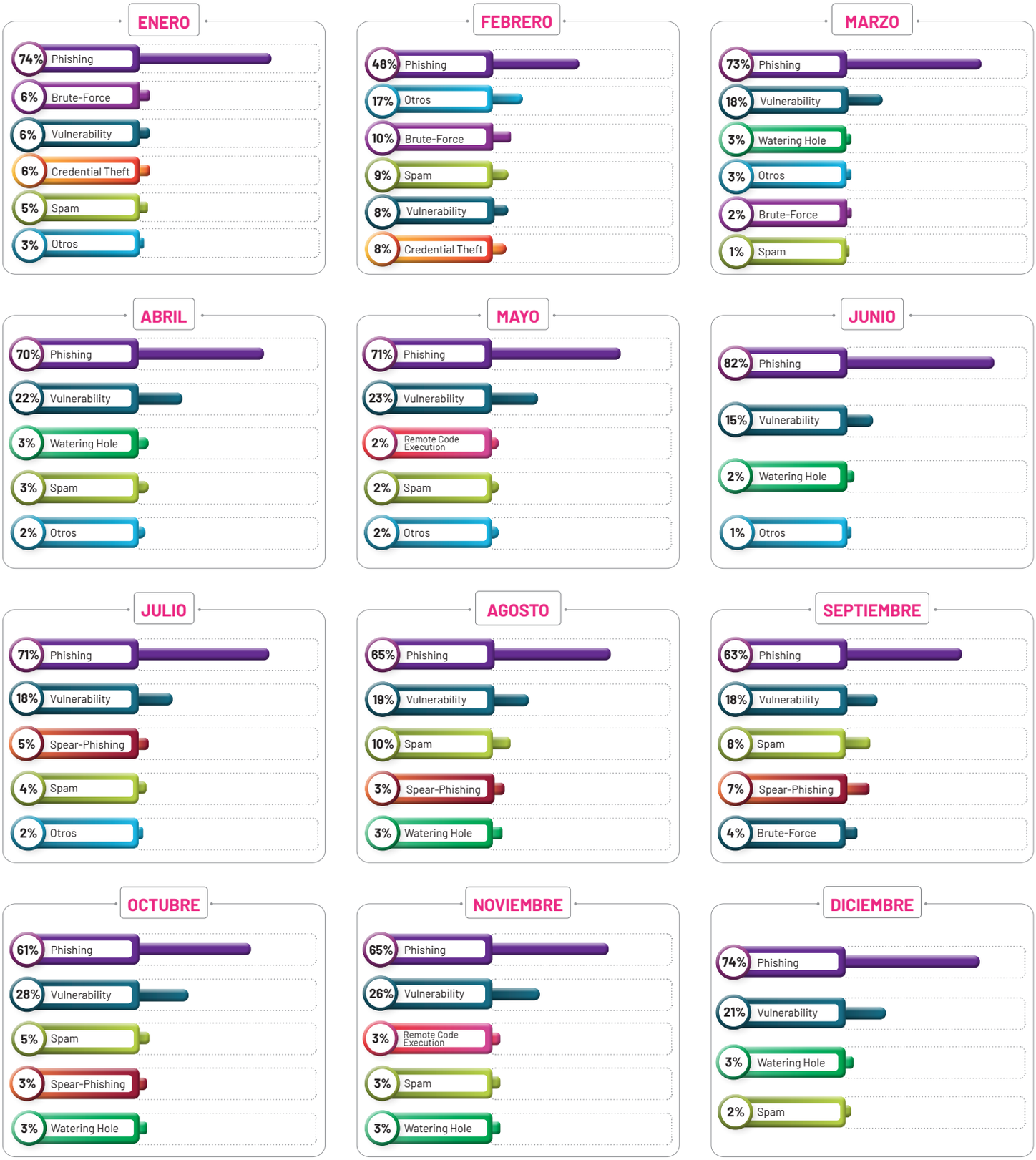
Es importante destacar las acciones y medidas que el Gobierno colombiano implementó para fortalecer la ciberseguridad, incluyendo:

- Actualización del CONPES de Ciberseguridad, con un enfoque en protección de infraestructuras esenciales.
- Refuerzo del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert), que mejoró su capacidad de respuesta y análisis de amenazas.

Colombia afrontó un 2024 desafiante en el mundo digital y los aprendizajes de este período serán clave para mejorar la ciberseguridad en los próximos años, por eso se deben tener en cuenta los siguientes aspectos:

- Una mayor inversión en tecnologías de detección avanzada y automatización.
- Mayor educación en ciberseguridad para usuarios y empresas.
- Cooperación internacional para combatir amenazas APT.

## Top vectores de ataque observados en 2024




*Gráfica 2. Top de vectores de ataques 2024. Fuente: CSIRT Financiero.*

# 6. Threat Intelligence Response

Inteligencia de amenazas y análisis de riesgos para la respuesta y remediación estratégica y operativa, cuyo proceso de identificar, analizar y actuar ante amenazas cibernéticas utiliza información detallada y actualizada sobre los actores de amenazas, sus métodos, herramientas y objetivos.

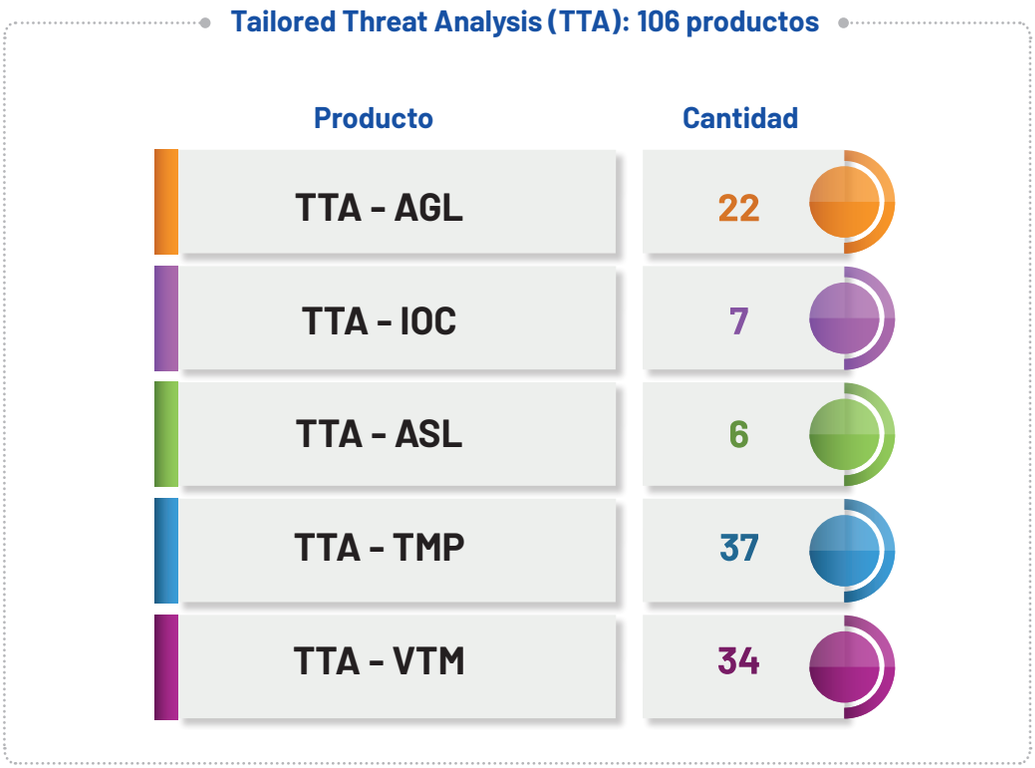
## 6.1 Threat Analysis & Modeling

El subservicio de Threat Analysis & Modeling brinda información sobre el análisis a múltiples amenazas que pueden afectar directa o transversalmente el sector financiero. Entre los productos que podemos encontrar en este subservicio se encuentran:

- **Cyber Security Warning:** reportes que se generan a partir del monitoreo diario de amenazas a través de fuentes públicas y privadas de información.
- **Tailored Threat Analysis:** informes técnicos sobre la cadena de infección de una amenaza en específico.
- **Monitoring Threat Analysis:** informes sobre la monitorización de la evolución de una amenaza, identificando patrones, comportamientos, actores de amenaza, indicadores de compromiso, tácticas y técnicas que puedan afectar a las organizaciones.
- **Threat Focus Report:** análisis enfocado hacia una amenaza en específico, teniendo en cuenta los riesgos que estos pueden generar para las infraestructuras tecnológicas de los asociados.

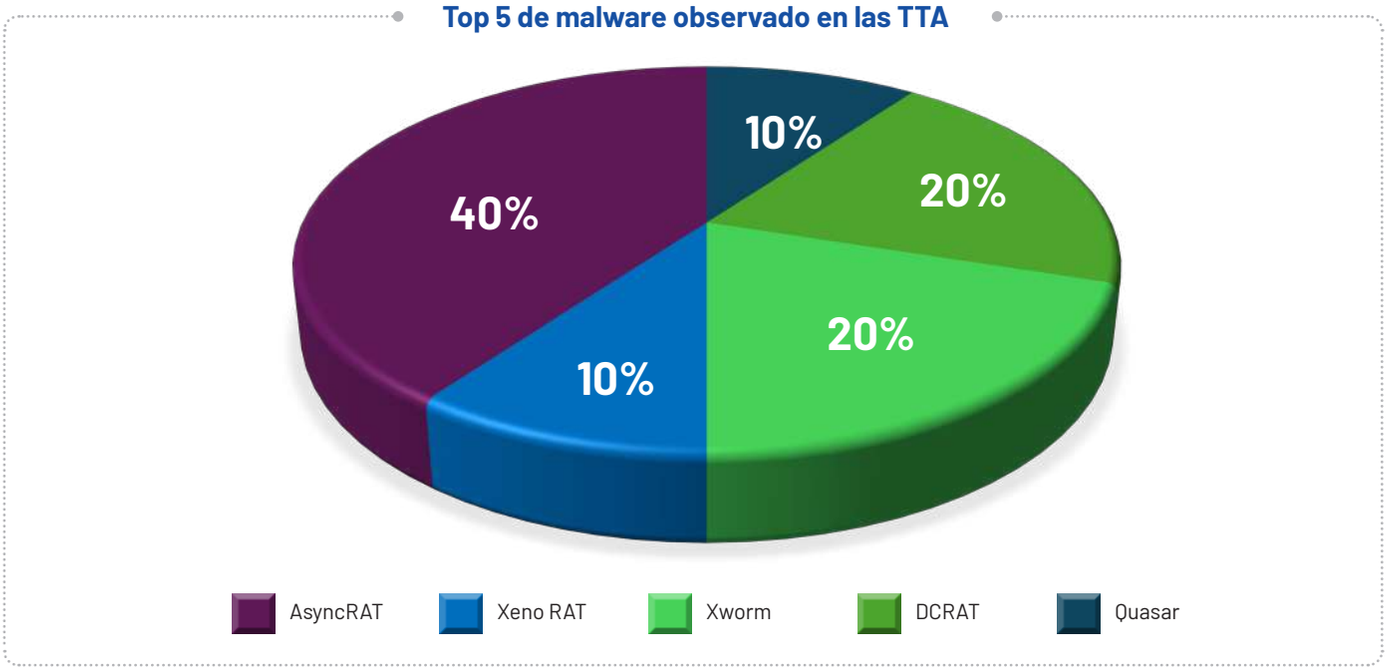
Durante el año 2024, el equipo del CSIRT Financiero generó varios productos relacionados con este subservicio.


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




***Gráfica 4.*** *Cantidad de Tailored Threat Analysis realizadas. Fuente: CSIRT Financiero.*

En el análisis de las amenazas identificadas en los productos del subservicio Tailored Threat Analysis (TTA), se detectó la recurrencia de varios malware, lo que permite establecer el top 5 de los más observados en 2024.




***Gráfica 5.*** *Top 5 de malware observados en productos TTA. Fuente: CSIRT Financiero.*

- **Monitoring Threat Analysis / Advanced Threat Report (MTA)**

A través de sus capacidades se realizaron dos (2) productos que presentan el análisis de distintas ciberamenazas que afectaron a diferentes sectores en Colombia y que pueden consultarse en el portal de asociados:

1. Análisis de amenazas encontradas en Deep y Dark Web (CRT_MTA_2024_001: julio 2024)
2. Amenazas distribuidas por Phishing en Colombia (CRT_MTA_2024_002: agosto 2024).

- **Threat Focus Report (TFR)**

El CSIRT Financiero generó nueve (9) Threat Focus Report, en los cuales analizó diversas ciberamenazas, como el ransomware y los grupos APT, que pueden afectar a las infraestructuras informáticas. Estos reportes pueden ponerse en operación mediante la implementación de las reglas Yara y Sigma incluidas en cada investigación. Igualmente, estos productos se encuentran disponibles en el portal de asociados para su consulta.

1. AsyncRAT (CRT_TFR_2024_001: enero de 2024).
2. APT HAFNIUM y su método de persistencia GhostTask (CRT_TFR_2024_002: enero de 2024).
3. Stealer para la captura y exfiltración de datos sensibles (CRT_TFR_2024_003: marzo de 2024).
4. Análisis a la técnica T1037.001 Boot or Logon Initialization scripts: Logon script (Windows) (CRT_TFR_2024_004: abril de 2024).
5. GULOADER (CRT_TFR_2024_005: julio de 2024)
6. Formbook (CRT_TFR_2024_006: septiembre de 2024).
7. Blackjack, Akira, y Bluebottle (CRT_TFR_2024_007: octubre de 2024).
8. Informe de SpyNote (CRT_TFR_2024_008: octubre de 2024).
9. Ransomware en Colombia (CRT_TFR_2024_009: diciembre de 2024).

## 6.2 Threat Security Response

- **Threat Uses Cases**

El equipo de analistas del CSIRT Financiero, trabaja continuamente en la elaboración de diferentes entregables, que sirven como insumo para los equipos de respuesta ante incidentes de sus asociados, gracias al entendimiento de las ciberamenazas y los actores maliciosos detrás de ellas, identificando estrategias de detección y mitigación.

Entre estos productos se encuentran los Threat Use Cases, cuya finalidad es dar a conocer las acciones necesarias que permitan detectar, contener y mitigar las amenazas del ciberespacio.

En el año 2024, el CSIRT Financiero generó un informe sobre AgentTesla, entregando medidas enfocadas en la identificación de este troyano en cada una de las fases del modelo de identificación y prevención de la actividad de intrusiones cibernéticas (Cyber Kill Chain).

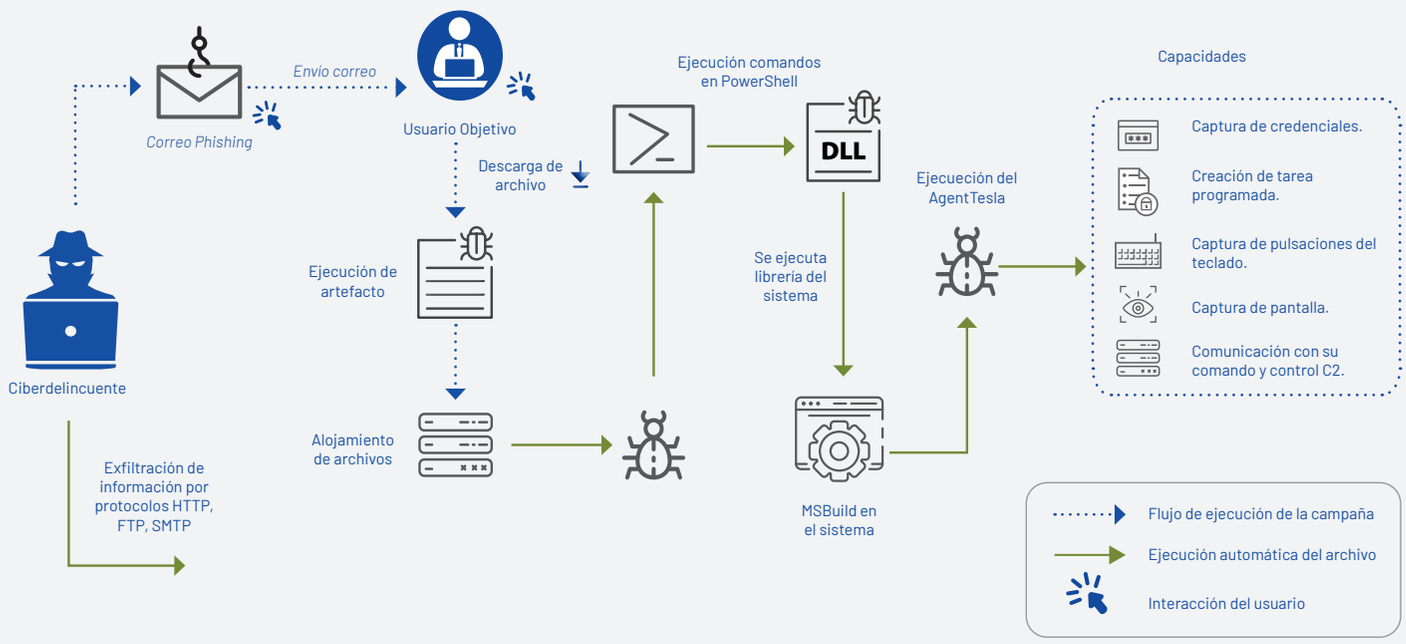
- Caso de uso para la detección, mitigación y contención de la amenaza conocida como AgentTesla, 26/08/2024.

AgentTesla mantuvo actividad constante en el ciberespacio en el año 2024, desplegando diferentes campañas maliciosas. Este troyano se distribuye a través de correos electrónicos de tipo phishing, utilizando archivos adjuntos como LNK, CHM, VBS, EXE o enlaces que redireccionan al usuario a sitios de alojamiento de artefactos, que posteriormente se ejecutan y liberan la carga maliciosa de esta amenaza.

Este troyano utiliza varios artefactos en su cadena de infección, entre los que destacan archivos de texto plano, ejecutables, imágenes y librerías (DLL), las cuales han sido modificadas por el actor de amenaza. Esta forma de operar es empleada por el troyano para evitar la detección por parte de soluciones antimalware del equipo.

En la siguiente imagen se puede apreciar el modelado del evento de AgentTesla, el cual se basa en las diferentes campañas analizadas por el Csirt Financiero:

**Modelado de amenazas: AgentTesla**




***Gráfica 6.*** *Modelado de la amenaza. Fuente: CSIRT Financiero.*

- **Incident Response Playbook**

Estos documentos conforman un conjunto de procedimientos que describen el paso a paso a seguir frente a un incidente de ciberseguridad, siendo una guía para los equipos de seguridad y de respuesta a incidentes en la identificación, contención, erradicación y recuperación de un incidente.

Estos entregables permiten una respuesta estructurada y eficiente ante las diferentes ciberamenazas, proporcionando un marco predefinido para proceder sin tener que improvisar, minimizando así, el tiempo de reacción al incidente y reduciendo los daños.

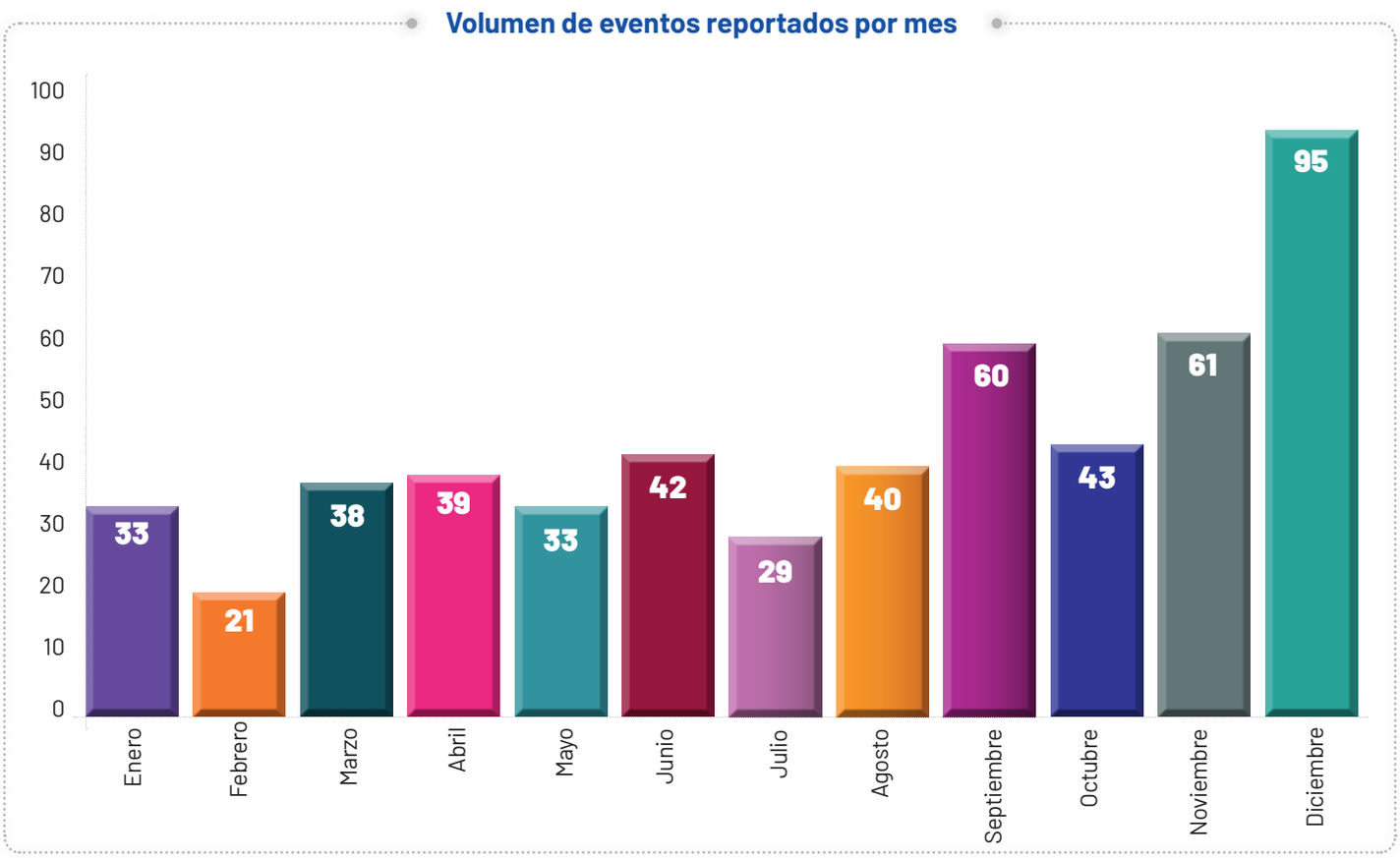
En la vigencia del año 2024, desde el CSIRT Financiero se desarrollaron dos (2) playbooks; uno orientado a la descripción de algunos de los mecanismos de persistencia empleados por los actores maliciosos y el segundo relacionado con el compromiso de cuentas de correo electrónico empresariales, Business Email Compromise (BEC).

A la fecha, el equipo de analistas del CSIRT Financiero ha generado 29 playbooks. Estos documentos están disponibles en el portal de asociados para su consulta en cualquier momento.

- **Support Incident Response**

A través del servicio de Support Incident Response, los asociados reportan al equipo técnico posibles eventos de seguridad presentados en sus infraestructuras tecnológicas. Entre estos reportes, destacan correos tipo phishing y spearphishing, archivos maliciosos relacionados con malware y suplantación de sitios o aplicaciones web de los asociados, entre muchas otras situaciones.

Durante 2024, se atendieron 534 incidentes a través del servicio Support Incident Response, los cuales están distribuidos de la siguiente forma:




***Gráfica 7.*** *Eventos reportados por los asociados. Fuente: CSIRT Financiero.*

Gracias a estas investigaciones, se ha obtenido información valiosa sobre las distintas familias de malware que afectan directamente al sector financiero en Colombia, con base en los incidentes reportados por los asociados.

En la gráfica a continuación, se puede observar que RemcosRAT, AsyncRAT y AgentTesla han estado presentes en más del 50% de los eventos reportados.

Es importante señalar, que AsyncRAT también se encuentra dentro del top 5 de los principales malware que han sido observados en diferentes campañas contra el sector financiero durante 2024.

**Familias de malware observadas en eventos reportados**

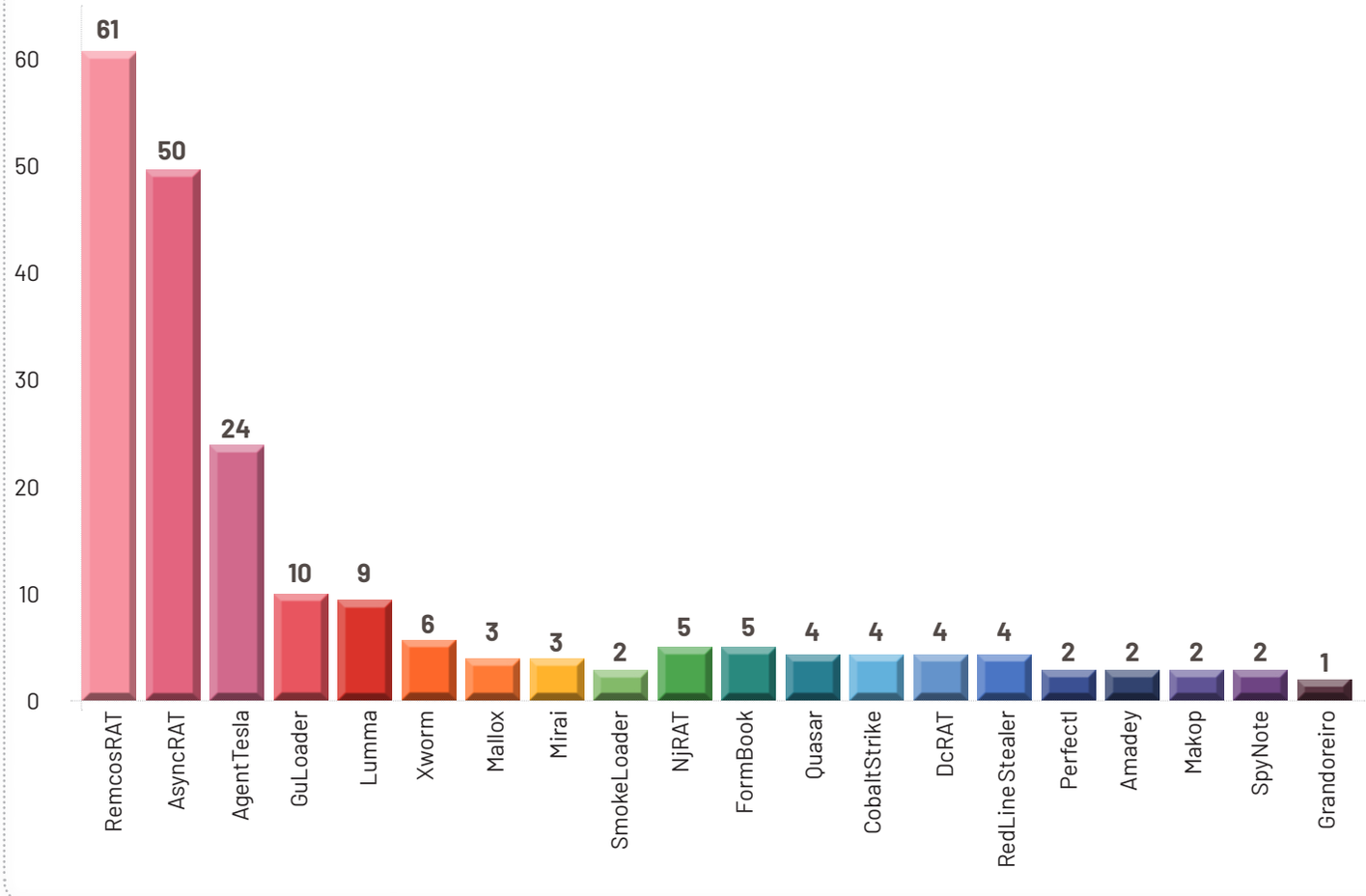



***Gráfico 8**. Familias de malware identificadas en 2024. Fuente: CSIRT Financiero.*

## Vectores de ataque

Durante el análisis de los 534 casos reportados por los asociados, se identificaron los vectores de ataque utilizados por los cibercriminales, siendo el empleo de malware, el phishing y la suplantación de sitios web, los más utilizados.


***Gráfica 9.*** *vectores de ataque utilizados por los cibercriminales. Fuente: CSIRT Financiero.*

Así mismo, como resultado de la actividad de monitoreo en la Deep y Dark Web, se identificaron cuentas comprometidas de colaboradores y clientes de diferentes entidades financieras, las cuales fueron reportadas y relacionadas en 234 productos.

## 6.3 Threat Detection & Prevent

- **Malware Activity**

Durante el año 2024, se desarrollaron diversas reglas YARA enfocadas en la identificación de múltiples familias de malware, distribuidas en varias categorías. Este desarrollo refleja el compromiso por mejorar las capacidades de detección frente a una amplia variedad de amenazas, abordando desde ataques dirigidos hasta campañas masivas.

**Identificación de familias mediante reglas YARA**

| Familia | Nº reglas YARA desarrolladas | Categoria |
|---|---|---|
| AgentTesla | 3 | RAT |
| Guloader | 3 | Loader |
| ELPACO | 3 | Ransomware |
| MrAnon | 2 | Stealer |
| DarkGate | 2 | Loader |
| NanoCore RAT | 2 | RAT |
| Chavecloak | 1 | Troyano Bancario |
| SamsStealer | 1 | Stealer |
| zgRAT | 1 | RAT |
| DarkTortilla | 1 | Loader |
| RisePro | 1 | Stealer |
| Coyote | 1 | Troyano Bancario |
| Xeno RAT | 1 | RAT |
| Blank Grabber | 1 | Stealer |
| Xworm | 1 | RAT |

***Gráfica 10 :*** *Familias de malware identificadas con reglas Yara. Fuente: CSIRT Financiero.*

*Las reglas YARA identifican y clasifican malware mediante patrones de texto, bytes o cadenas en archivos y procesos.*

## • Unified Threat Identification

Se desarrollaron diversas reglas SIGMA enfocadas en la detección de amenazas dirigidas al sector financiero. Estas reglas abarcan múltiples familias de malware utilizadas en ataques contra entidades financieras, permitiendo una detección más efectiva. Gracias a este desarrollo se fortaleció la capacidad de respuesta ante amenazas como troyanos bancarios, loaders y RATs, contribuyendo a la protección de infraestructuras críticas y la mitigación de riesgos en operaciones financieras.

### Identificación de familias mediante reglas SIGMA

| Familia | Nº reglas SIGMA desarrolladas | Categoria |
|---|---|---|
| Xeno RAT | 1 | Rat |
| RisePro | 1 | Stealer |
| Ousaban | 1 | Troyano bancario |
| XWorm | 1 | Rat |
| coyote | 1 | Troyano bancario |
| strRAT | 1 | Rat |
| Loki Locker | 2 | Ransomware |
| AgentTesla | 2 | Rat |
| Bumblebee | 2 | Loader |
| GuLoader | 2 | Loader |
| Tarrask | 2 | Herramienta |
| DarkGate | 3 | Loader |

*Las reglas SIGMA detectan actividades sospechosas en los registros (logs) de sistemas mediante comportamientos.*

***Gráfica 11:*** *Familias de malware identificado con reglas Sigma. CSIRT Financiero.*

- **Suricata**

Suricata es un potente motor de detección y prevención de intrusiones (IDS/IPS) que permite identificar tráfico malicioso en tiempo real, mediante análisis profundo de paquetes (DPI) y reglas basadas en firmas, incluyendo compatibilidad con Snort. Su arquitectura permite inspeccionar grandes volúmenes de tráfico, detectar amenazas en protocolos clave como HTTP, DNS y SMB.

Además, Suricata puede operar en modo IPS para bloquear ataques, integrarse con sistemas de correlacionador de eventos y extraer metadata de red.

En 2024, el equipo del CSIRT Financiero, generó una regla suricata para la identificación de malware que se ha visto en diferentes campañas en Colombia, como AgentTesla, AsyncRAT, FormBook, GuLoader y NjRAT, ayudando a la identificación del tráfico de red que generan estas amenazas.

- **Network Threat - Snort, IPtables**

Entre los sistemas de detección de intrusiones en la red más conocidos y eficaces se encuentra Snort, tecnología capaz de realizar análisis de alto nivel al tráfico de red, de protocolos y búsqueda de contenido en tiempo real. Este sistema de detección de intrusos en la red permite implementar reglas que contribuyen a identificar anomalías y posibles ataques como, por ejemplo, denegación de servicio, desbordamiento de búfer o escaneo de puertos, entre otros. Al detectar comportamientos sospechosos se envía una alerta en tiempo real.

Por otro lado, los sistemas Linux cuentan con IPtables, herramienta del firewall que ayuda a controlar el tráfico de red, estableciendo qué conexiones se pueden habilitar y cuáles se pueden bloquear según los criterios definidos por la organización.

Las reglas IPtables son instrucciones utilizadas en sistemas operativos basados en Linux, están organizadas en tablas y cada tabla contiene cadenas que definen conjuntos específicos de reglas.

El portal de asociados cuenta con un módulo que permite la creación automática de reglas Snort e IPtables. Con esto se busca brindar una capa adicional de seguridad a las infraestructuras tecnológicas de los asociados, abordando tanto la detección de amenazas como el control de acceso a nivel de red.

## 6.4 Threat Intelligence Exchange

El intercambio de inteligencia de amenazas es un proceso mediante el cual, las entidades del sector financiero de Colombia y el CSIRT Financiero comparten información sobre ciberamenazas, ataques y vulnerabilidades. El objetivo es fortalecer la ciberseguridad de la comunidad en general, permitiéndoles anticiparse y responder de manera efectiva a las amenazas emergentes que puedan afectar al sector, tanto de manera directa como transversal.

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

- **Detección temprana de amenazas:** permite a las entidades financieras conocer, de manera anticipada, las tácticas, técnicas y procedimientos (TTP) utilizados por los ciberdelincuentes y el malware asociado a los diferentes ataques realizados.

- **Mejora de la defensa:** al recibir información detallada sobre nuevas amenazas, las entidades pueden ajustar y mejorar sus medidas de seguridad para hacer frente a las tácticas emergentes.

- **Colaboración sectorial:** el intercambio de inteligencia permite a las entidades financieras colaborar entre sí, compartiendo experiencias y estrategias para hacer frente a amenazas comunes que pueden afectar al sector financiero en Colombia.

- **Reducción de riesgos:** al estar al tanto de las amenazas actuales, las entidades pueden tomar medidas proactivas para reducir la exposición a riesgos financieros y reputacionales.

El CSIRT Financiero cuenta con la plataforma MISP (Malware Information Sharing Platform) mediante la cual se correlacionan indicadores de compromiso (IOC), técnicas, tácticas y procedimientos (TTP) con el fin de compartir inteligencia de amenazas; automatizando el consumo de esta información en las diferentes plataformas de las entidades financieras.

MISP (Malware Information Sharing Platform) es una plataforma colaborativa diseñada para fortalecer la ciberseguridad a través del intercambio estructurado de inteligencia de amenazas. Permite la correlación automática de Indicadores de Compromiso (IOC) y patrones de ataque, facilitando una detección proactiva y una respuesta más rápida ante ciberamenazas. Su enfoque en la automatización y el trabajo en comunidad la convierte en una herramienta esencial para anticiparse a riesgos y mejorar la resiliencia digital.

En el ecosistema financiero, donde la ciberseguridad es clave para proteger la integridad de las transacciones y la confianza de los clientes, estar conectado a MISP es una ventaja estratégica. La conexión bidireccional permite, no solo recibir inteligencia de amenazas en tiempo real, sino también compartir indicadores clave sobre ataques dirigidos al sector. Esta colaboración fortalece la detección de fraudes, la mitigación de riesgos y la respuesta ante incidentes, permitiendo a las entidades financieras anticiparse a nuevas amenazas y reforzar la seguridad de sus plataformas y servicios digitales, de la mano del CSIRT Financiero.

El CSIRT Financiero mantiene la integración de nuestra instancia MISP con 15 entidades financieras; permitiéndoles obtener indicadores de compromiso de manera inmediata, reduciendo la carga y tiempos operativos.

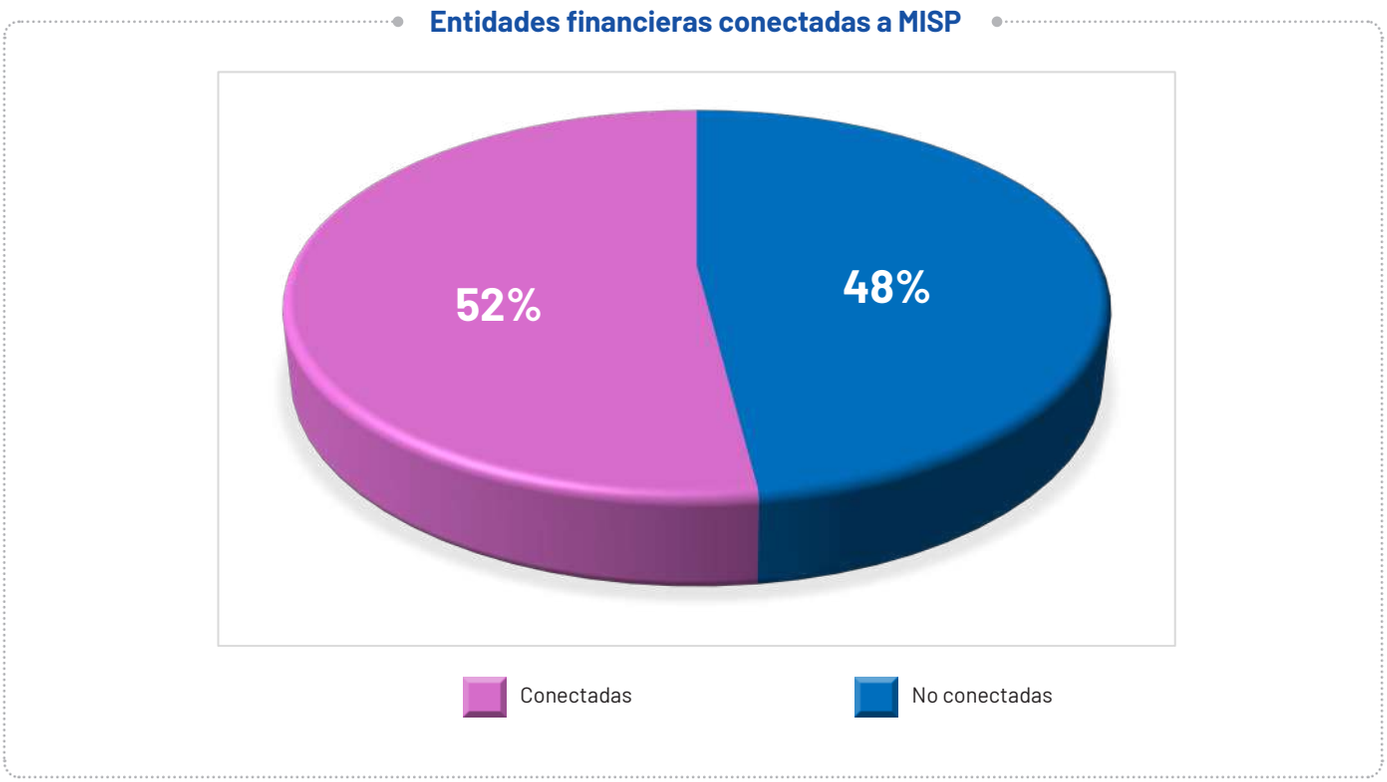



*Gráfico 12. Entidades conectadas a MISP. Fuente: CSIRT Financiero.*

En 2024 dos nuevas entidades se unieron, finalizando el año con treinta y una (31). Del total anterior se encuentran quince (15) conectadas a nuestra instancia MISP a través de diferentes tecnologías como: SOAR, MISP, TIP y XDR.

- **Advanced Threat Emulation**

La emulación de malware tiene como fin simular el comportamiento de una amenaza que pueda afectar de manera directa o indirecta al sector financiero, permitiendo a las entidades financieras, evaluar la efectividad de sus medidas de seguridad existentes frente a la detección y mitigación de posibles ciberamenazas.

En 2024, se realizaron dos emulaciones asociadas con tipos de malware presentes en campañas vistas en Colombia.

- Emulación de la técnica Hidden Task CRT-ME-2024-004: **febrero 2024**
- Component Object Model Hijacking CRT-ME-2024-002: **agosto 2024**

## 6.5 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, adaptándose 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, anticipándose a las amenazas y garantizando una respuesta eficaz frente a los riesgos cibernéticos.

- **Strategy CTI Office**

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 permita anticipar y mitigar riesgos de seguridad.

En este período, se distribuyeron (12) Security Bulletin 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 Bulletin, 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.

- **Webinars**

Con el objetivo de fortalecer las capacidades de nuestros asociados y fomentar una cultura de seguridad más robusta, lanzamos tres nuevos formatos de entrenamiento y divulgación en ciberseguridad. Estas iniciativas, diseñadas para mejorar el conocimiento y la preparación frente a amenazas emergentes, permitieron a los participantes adquirir herramientas prácticas, compartir experiencias y mantenerse actualizados en un entorno en constante evolución.

- **CSIRT Training:** espacios de formación, tanto virtuales como presenciales, con un enfoque práctico (hands-on), diseñados para que los participantes adquieran habilidades técnicas aplicables a su entorno. Estas sesiones fomentan el intercambio de mejores prácticas y proporcionan herramientas metodológicas clave para enfrentar desafíos en ciberseguridad.

- **CSIRT Experiences:** encuentros virtuales que facilitan el intercambio de experiencias entre entidades del sector financiero, expertos en ciberseguridad y organizaciones externas. A través del análisis de incidentes reales, los participantes extraen lecciones valiosas para fortalecer la resiliencia y mejorar la seguridad en sus organizaciones.

- **CSIRT Cyber Webinar:** espacios virtuales con la participación de expertos internacionales, enfocados en tendencias y actualizaciones clave en ciberseguridad. Estas sesiones proporcionan información estratégica y práctica para fortalecer la seguridad y mejorar la capacidad de respuesta ante amenazas emergentes.

Adicionalmente se realizaron diez (10) webinar que permitieron a nuestros asociados entender y comprender, de forma estructurada, los riesgos y desafíos de la era digital. Además, al compartir conocimientos y estrategias de protección, se fortaleció la confianza de las entidades financieras reafirmando su compromiso con la ciberseguridad.

**Espacios de entrenamiento y divulgación en ciberseguridad**

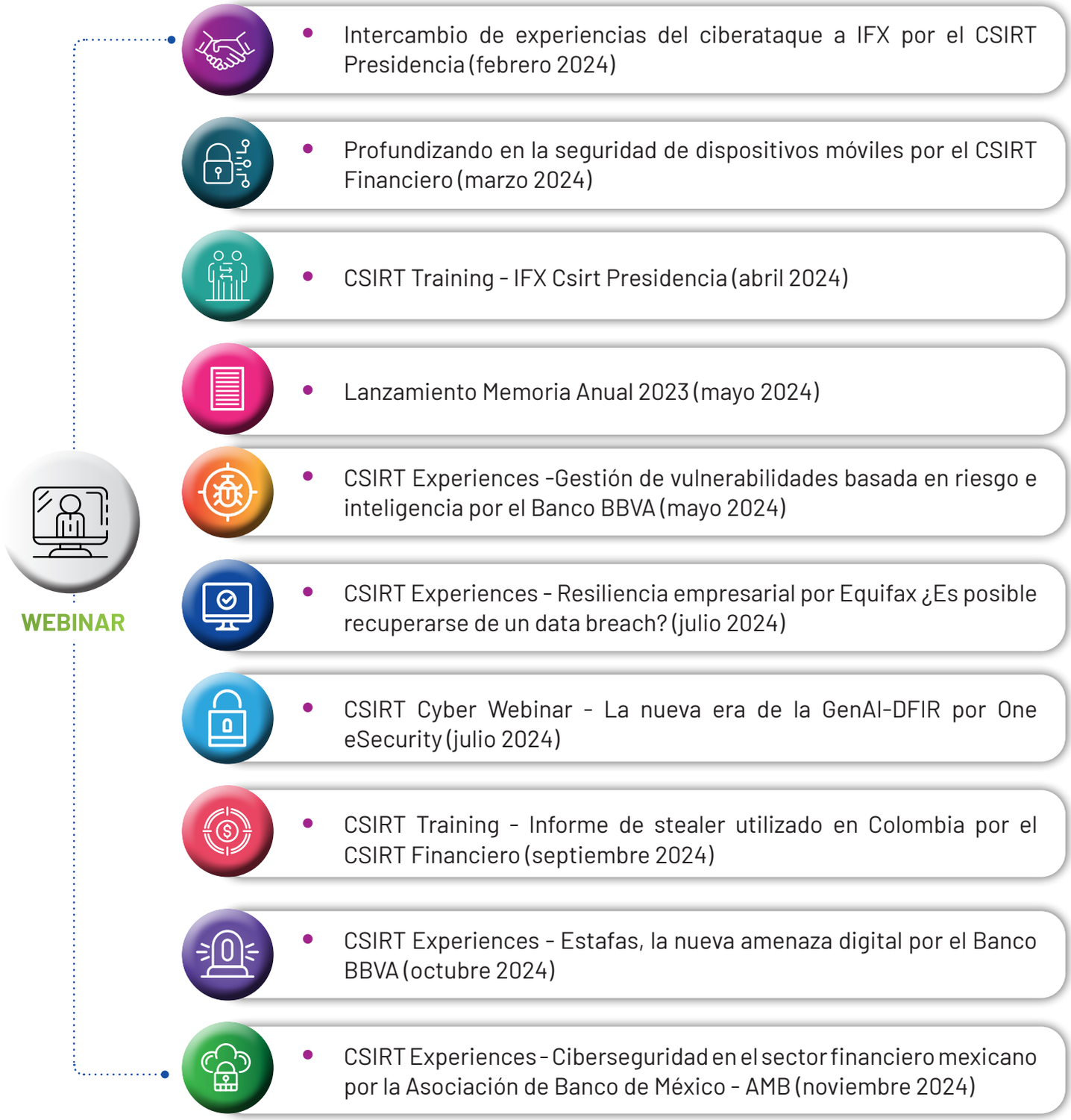



***Gráfico 13.*** *Webinar realizados el 2024. Fuente: CSIRT Financiero de acuerdo con el consecutivo.*

- **APT Monitor & Analysis Impact**

Una de las actividades más preocupantes observadas durante 2024 es la proliferación de grupos APT en la región. Éstos se caracterizan por su capacidad de operar durante períodos prolongados, evadiendo la detección y extrayendo datos sensibles de alta importancia estratégica. La presencia de estos grupos en Colombia podría estar relacionada con intereses geopolíticos, industriales y financieros de diversas naciones, lo que eleva el riesgo para sectores clave, como el gobierno, las infraestructuras críticas y las empresas de tecnología.


**Actividad grupos APT en la región**

| Nombre Grupo APT | Acciones en 2024 |
|---|---|
| Ransomhub | 4 |
| Lazarus | 4 |
| FIN7, ATK32 | 3 |
| APT-43, Kimsuky | 3 |
| APT-C-36, Blind Eagle | 3 |
| BlackCat, ALPHV | 3 |
| TA558 | 2 |
| RA World | 2 |
| Black basta | 2 |
| STORM-1575 | 1 |

***Gráfico 14.*** *Actividad grupos APT en la región. Fuente: CSIRT Financiero.*

- **Relevant Event**

Se identificaron 34 grupos de cibercriminales activos en Latinoamérica, empleando tácticas predominantes como el phishing y la explotación de vulnerabilidades. Estas amenazas han afectado significativamente al sector financiero, destacándose los siguientes eventos:

- **Ransomhub:** Responsable de más de 600 víctimas, este grupo utiliza un modelo de ransomware como servicio (RaaS) enfocado en comprometer todo tipo de entidades.

- **FIN7:** Introdujo el cryptor AvNeutralizer, diseñado para evadir soluciones antimalware, facilitando la infección de sistemas críticos y la distribución de malware sin que sea detectado.

- **APT-C-36 (Blind Eagle):** Dirigió campañas en Colombia y Ecuador, orientadas principalmente, a instituciones financieras y gubernamentales.

- **Kimsuky:** Desarrolló dos nuevos malware destinados a campañas de phishing, demostrando una evolución constante en sus capacidades, además de incluir nuevas variantes de ransomware a su arsenal de herramientas.

- **APT29:** Llevó a cabo una campaña que comprometió a más de 200 víctimas, explotando el protocolo RDP y diversas vulnerabilidades en sistemas desactualizados.

- **Storm1575:** Ejecutó múltiples campañas de phishing, dirigidas tanto a usuarios corporativos como a entidades del sector financiero.

# 7. Tendencias en ciberseguridad 2025

La industria bancaria continúa en proceso de transición hacia una digitalización efectiva y segura, impulsada por la proliferación de ciberamenazas cada vez más complejas y sofisticadas, y por la necesidad de alinearse con las expectativas y demandas de los clientes.

Este nuevo escenario cibernético está transformando las estrategias y modelos operativos de las entidades financieras, que exige estar a la vanguardia de las nuevas tecnologías. Un mercado tan competitivo y atractivo para los cibercriminales, debe estar preparado para lidiar con los desafíos y amenazas que están por venir durante este 2025.

## 7.1 Tendencias en el sector financiero

### 1. Cloud banking: nuevos vectores de ataque

A través de este modelo tecnológico, las entidades bancarias utilizan servidores remotos de proveedores externos para alojar su infraestructura y prestar sus servicios y productos. Esta nueva arquitectura simplifica y agiliza las operaciones bancarias, a la vez que reduce los costes derivados del almacenamiento de datos.

Aunque la migración de los bancos hacia tecnologías en la nube lleva años en proceso, se prevé que para el 2025, aumente el número de entidades que utilicen infraestructuras basadas en la nube o bien, adopten modelos híbridos.

Sin embargo, esta transformación digital supone, además, nuevos riesgos en materia de ciberseguridad, ya que la arquitectura en la nube aumenta la superficie de ataque con nuevas vulnerabilidades, cada vez más complejas.

Un ejemplo que evidencia esta nueva amenaza es el ciberataque perpetrado en 2023 contra una multinacional proveedora de servicios en la nube, con sede en Bogotá, que logró interrumpir la actividad de varias instituciones estatales y privadas de diferentes países latinoamericanos, entre ellos Colombia, uno de los principales afectados.

Y, según un estudio realizado por PwC, los riesgos relacionados con los servicios en la nube son una de las principales preocupaciones para los directivos y responsables de tecnología de las empresas latinoamericanas.

Entre las principales vulnerabilidades figuran:

**Controles de acceso mal configurados**

**Almacenamiento de datos no seguro**

**Configuraciones incorrectas**

## 2. Avances en la Inteligencia Artificial

La inteligencia artificial ha sido una de las principales revoluciones tecnológicas de los últimos años. Algunas de las aplicaciones de esta disciplina, como el procesamiento de lenguaje natural o la automatización de procesos, han transformado el modo de operar de las entidades bancarias, desde la hiperpersonalización de catálogo de productos hasta la detección de fraudes y tendencias del mercado.

No obstante, se prevé que durante este 2025, se sigan perfeccionando las capacidades de la Inteligencia Artificial y estas sean adoptadas a gran escala, siendo cada vez mayor el número de entidades del sector que la integren en sus operaciones.

La implementación de tecnologías de la IA conlleva ciertos riesgos, destacando entre ellos su vulnerabilidad ante los ataques de 'contaminación', también conocidos como 'data poisoning', consistentes en la manipulación de conjuntos de datos de entrenamiento de un sistema de Inteligencia Artificial para introducir elementos maliciosos y comprometer el modelo.

Aunque la 'contaminación' de datos en sistemas de aprendizaje automático no representa una novedad, el auge de tecnologías como los modelos lingüísticos de gran tamaño (LLM) que requieren un importante volumen de datos de entrenamiento, está provocando que este tipo de ataques cobren cada vez más protagonismo.

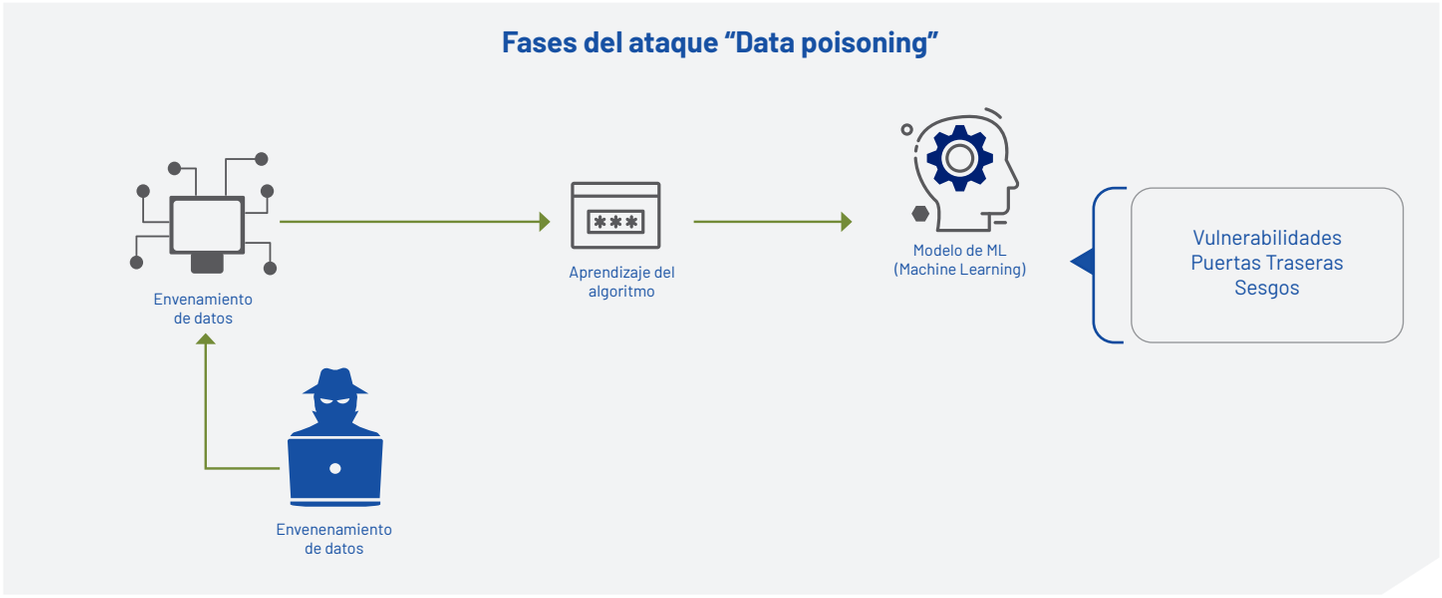



***Gráfico 15.*** *Fases del ataque "Data poisoning". Fuente: CSIRTFinanciero.*

## 3. Smartphones en el punto de mira

Otra de las amenazas que se proyectan para el 2025 son los ataques dirigidos a los teléfonos inteligentes, conforme disminuyen los malware tradicionales a ordenadores. Se trata de una tendencia ya detectada en 2024 y que se espera que perdure durante este año.

Se han detectado una serie de malware bancarios dirigidos a dispositivos móviles cuya prevalencia se prevé que continúe durante el año 2025 y de los que desde el CSIRT Financiero se han elaborado varios productos:

### Toxicpanda

Se trata de un troyano bancario que afecta a teléfonos Android. Permite a los atacantes captar contraseñas de un solo uso o aplicaciones de autenticación. Su objetivo principal es realizar transferencias desde los dispositivos infectados mediante la intervención de cuentas a través de la técnica conocida como On-device fraud (ODF).

- [AGL] Análisis técnico a ToxicPanda
- [CSW] Nuevo troyano bancario denominado "ToxicPanda" afecta a Europa y América del Sur

## Grandoreiro

Este software malicioso continúa activo a pesar de la detención de algunos de los integrantes del grupo que lo desarrollaron. Recientemente, se han detectado nuevas variantes y actualizaciones de este malware que dificultan su detección, por ejemplo, utilizando nuevas técnicas para pasar desaparecido ante las medidas de seguridad de las entidades bancarias, como algoritmos para la generación de direcciones web falsas y el cifrado de los datos sustraídos. También hay indicios de que podría estar ejecutándose bajo el modelo de Malware as a Service (MaaS), aunque estaría limitado a un grupo reducido de cibercriminales.

- [TTA] Campaña que distribuye troyanos brasileños en Colombia
- [CSW] Nuevos detalles sobre el troyano bancario Grandoreiro
- [CSW] Nueva actividad del troyano bancario Grandoreiro
- [CSW] Nuevas Actividades Maliciosas del Troyano Bancario Grandoreiro
- [CSW] Nuevas Actividades Maliciosas del Troyano Bancario Grandoreiro

## DroidBot

Este troyano de acceso remoto (RAT) también está dirigido a dispositivos Android, y emplea distintas técnicas de superposición y VNC oculto, con capacidades similares a las de los de un "spyware", permitiendo así a los atacantes interceptar las interacciones del usuario. Hasta la fecha, tiene como objetivo 77 entidades diferentes entre ellas instituciones bancarias y casas de cambio de criptomonedas. Se han detectado campañas activas principalmente en países europeos, pero se espera que comience a extenderse su distribución en América Latina.

- **[CSW] Nueva amenaza móvil:** DroidBot y su impacto en el sector financiero

### 4. Inclusión financiera: un paso más hacia la igualdad de oportunidades

Uno de los principales desafíos de esta industria es potenciar la bancarización y favorecer el acceso a los servicios financieros, integrando así a nuevos consumidores en la economía digital. La tecnología móvil constituye una de las claves para esta expansión, ya que permite a los usuarios realizar diversidad de transacciones bancarias, como pagos desde un dispositivo móvil, uno de los más comunes. No obstante, superar esta brecha de inclusión financiera y democratizar los servicios bancarios aumenta el vértice de exposición.

Poner a disposición de los consumidores los servicios bancarios aumenta el riesgo de ciberataques si no se les proporciona paralelamente el conocimiento y la capacitación suficientes para adoptar decisiones informadas sobre el uso seguro de estos productos.

## 7.2 Tendencias en el sector tecnológico

### 1. Computación Cuántica

El año 2025 ha sido considerado como el año internacional de la ciencia y la tecnología cuántica, por lo que se espera un aumento considerable de la inversión en innovación en este aspecto tecnológico.

En el futuro, la computación cuántica promete ser un avance revolucionario transversal a la vida cotidiana y a los distintos sectores profesionales. Cuando se haya terminado de desarrollar, en la banca, la computación cuántica promete revolucionar el sector, tanto de forma negativa como positiva.

Esta dualidad se debe a que, si bien las innovaciones en computación cuántica pueden implicar la creación de nuevos paradigmas criptográficos, lo que actuaría como una amenaza importante para la seguridad de la información y de las transacciones del sector, pudiendo ejercer como herramienta para la ruptura de patrones cifrados hasta ahora seguros.

La computación cuántica también promete ser una oportunidad para optimizar y depurar procesos, mejorar la detección de fraude mediante 'quantum machine learning' o reducir la incertidumbre en las simulaciones, permitiendo ver más lejos y con menos errores.

### 2. Consolidación de Linux en el sector bancario

La arquitectura digital de los distintos organismos bancarios es antigua y se moderniza a través de actualizaciones que la modifican sin sustituirla, sin embargo, el código abierto, en especial el sistema operativo Linux, ha ido ganando terreno en este sentido y sustituyendo a sistemas operativos antiguos y desgastados.

La implementación de Linux en sustitución de los tradicionales sistemas de UNIX y Windows implica un beneficio para la digitalización de las empresas al permitir implementar gran cantidad de soluciones de código abierto que permiten mayor flexibilidad.

Los efectos del reemplazo de las infraestructuras digitales de las organizaciones bancarias a priori pueden suponer un reto, ya que obligan a la adaptación de personas y procesos a nuevos entornos digitales, sin embargo, puede suponer un avance significativo en la securitización de éstos, ya que abre nuevas oportunidades de explotar los sistemas y evitar ciberamenazas.

## 3. Hibridación de la banca digital y física

Aunque la tendencia actual es la digitalización de la banca, cada vez más sectores de población, incluyendo la más joven, requieren un contacto más próximo por parte de las entidades financieras.

Por tanto, es probable que la tendencia continúe hacia una hibridación entre digitalización y contacto personal, en lo que en el sector se ha denominado "banca figital".

En este sentido, es importante destacar que tendrá más éxito la compañía que consiga aunar las ventajas de la digitalización (inmediatez, accesibilidad remota...) y del plano físico (contacto personal, asesoramiento...).

Esta tendencia tiene que ver con los resultados arrojados por recientes estudios, donde se ha identificado que más del 50% de los encuestados quiere que los bancos ofrezcan un modelo que combine ambas formas de atención, esta tendencia es muy acusada entre los más jóvenes, donde se percibe la sucursal bancaria como un elemento que aporta confianza.

Aunque a priori el aumento de las transacciones físicas implica un descenso de los riesgos cibernéticos, la necesidad de inmediatez puede generar que los procesos estén menos securitizados y a la larga, podría implicar un aumento de los ataques basados en ingeniería social contra los trabajadores bancarios y los clientes.

## 4. Monedas digitales de los bancos centrales

Se está produciendo un auge de la presencia de monedas digitales emitidas por bancos centrales o CBDC (Central Bank Digital Currency), claro ejemplo de ello son el yuan digital (ya estandarizado) y el euro digital (en fase de estudio).

Según un estudio de 2021 realizado por BIS 9 de cada 10 Bancos Centrales se encontraban explorando de forma activa la incorporación de CBDC, y el 26% de los Bancos Centrales ya se encontraba desarrollando pruebas piloto.

Se pretende, con la adopción de las CBDC, agilizar las transacciones en espacios internacionales, sin embargo, su implementación por parte de potencias económicas globales y espacios regionales amplios pueden devaluar el dinero de otras regiones menos cohesionadas y de países con menor relevancia económica.

Aunque esta medida puede implicar grandes beneficios como la securitización y rapidez transaccional, especialmente en transferencias que involucren varias divisas; los efectos nocivos para otros espacios geográficos pueden producir crisis económicas regionales.

MEMORIA ANUAL

2024

**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

Santiago Rodríguez Varón

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

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

Aso Ban Caria