CSIRT FINANCIERO

MEMORIA ANUAL 2020

MAYO DE 2021

ASOBANCARIA

Construyendo la **Confianza** y **Solidez** del sector financiero

Resumen Ejecutivo

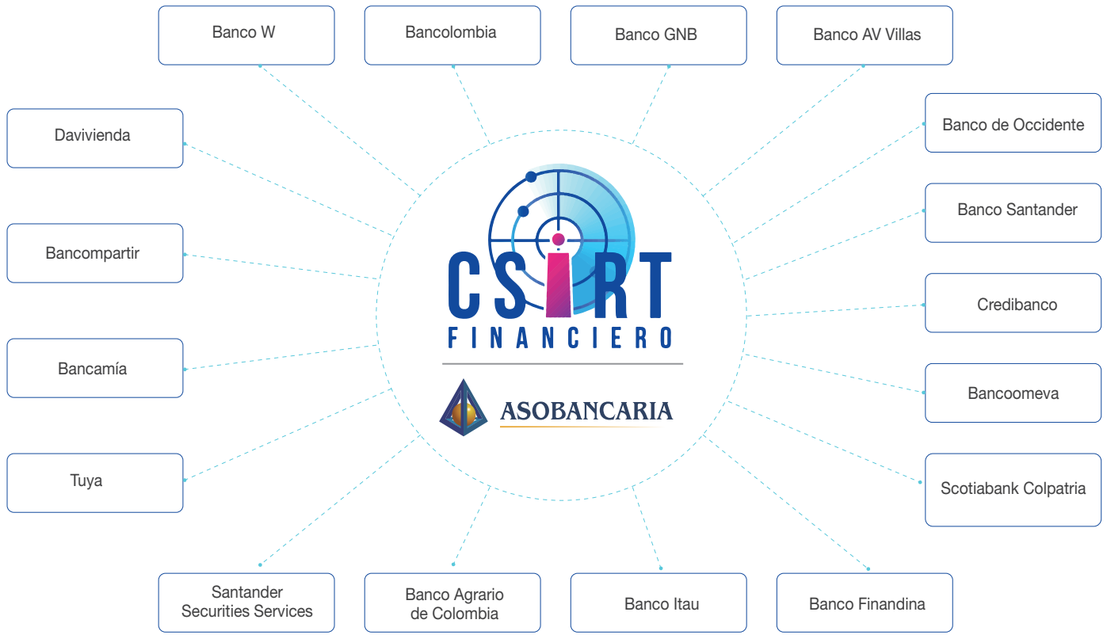
CSIRT Financiero
Hitos Memoria Anual 2020

• Seguimos creciendo para prevenir y anticipar riesgos cibernéticos en el sector

El equipo CSIRT sigue creciendo y ha sumado nuevos miembros que representan, no sólo a las entidades bancarias, sino al ecosistema financiero para madurar las capacidades de respuesta conjuntas ante las crecientes y dinámicas amenazas del ciberespacio. Hoy, el 85% del sector está conectado a la red de intercambio de información en línea.

Hoy consumen e intercambian información en línea
19 entidades financieras como miembros del CSIRT, redes y autoridades nacionales

Entidades Financieras (85% del sector activo en la comunidad)



- Recibimos acreditación de calidad de la comunidad global -FIRST, sello de calidad global con más de 500 equipos de ciberseguridad alrededor del mundo.

- **Vigilancia digital y prevención del ciber fraude durante la pandemia:**

  CSIRT Financiero ha entregado a las entidades bancarias alertas e información técnica en línea, alertando a los agremiados sobre nuevos riesgos digitales, nuevas tipologías de ciber fraude y recomendaciones de seguridad en el marco de la pandemia.

- **Fortalecimos la red de intercambio global y regional:**

  Seguimos sumando esfuerzos con otros CSIRT de referencia internacionales, entidades multilaterales, ISACs (Information Sharing and Analysis Centers), equipos de investigación, a nivel regional con Asociaciones Bancarias, autoridades locales, otros sectores, líderes tecnológicos y centros de investigación de amenazas cibernéticas para contar con más y mejor información.

Microsoft aws CYBER THREAT ALLIANCE

A lo largo de 2020, el Csirt Financiero ha trabajado constantemente para identificar todas aquellas ciberamenazas que han rodeado al sector financiero y que han puesto en riesgo la integridad de las entidades; todo esto enmarcado en un un panorama de constante cambio y adaptación. A continuación, se pueden observar los trabajos realizados por el Csirt Financiero con el objetivo de prevenir las diversas ciberamenazas identificadas en el sector:

510 **Alertas realizadas**
Las 510 alertas se enmarcan dentro del pilar del Observatorio de Ciberseguridad.

5.884 **IOCS Suministrados**
Los IOCs suministrados corresponden en su mayoría a troyanos y grupos APT que afectan al sector financiero.

510 **Documentos generados**
Lo que corresponde a Boletines Mensuales, informes Monográficos de Amenazas, Alertas, Playbooks y Case Study.

48 **Alertas inteligencia de amenazas**
Con la función de prevenir ciberamenazas respecto al sector financiero.

61 **Reglas**
Repartidas entre 18 reglas YARA y 43 reglas Sigma.

193 **Peticiones Apoyo a incidentes**
Fomentando la colaboración entre CSIRT y los asociados así como la capacidad de respuesta del equipo.

6 **Playbooks y Case Study**
Divididos en 5 Playbooks y 1 Case Study disponibles para los asociados.

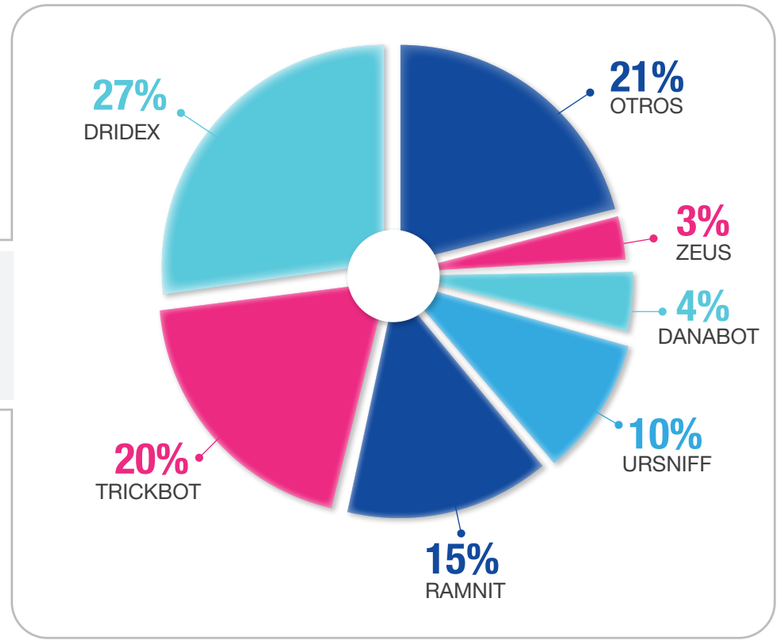
Dentro del Observatorio de Ciberseguridad del Csirt Financiero, se han tratado las ciberamenazas de manera pormenorizada en alertas, boletines, informes o monográficos. De todos estos documentos se desprenden análisis y tendencias que han marcado el 2020 y que se recogen a continuación.

- SPAM Y PHISHING
- DOMINIOS MALICIOSOS
- RANSOMWARE Y DDoS
- MALWARE DE RECOLECCIÓN
- EXPLOTACIÓN DE VULNERABILIDADES

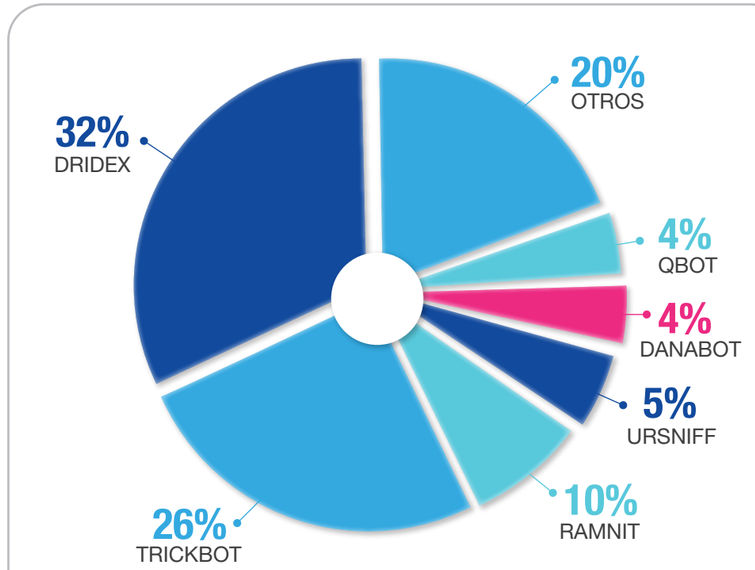
Observatorio de Ciberseguridad

Sobre los **Troyanos bancarios**, su uso se ha **incrementado**, tanto aquellos diseñados para afectar a **ordenadores**, como los dirigidos contra **dispositivos móviles.** En términos generales, los principales troyanos identificados en 2020 se recogen a continuación:

Top Troyanos bancarios Global



Top Troyanos bancarios América



Un aspecto para destacar ha sido la aparición de múltiples troyanos bancarios de origen brasileño que han afectado a entidades financieras. A lo largo del año se ha identificado:

- Notable **incremento en su uso**
- Mayor **sofisticación**

En su mayoría, emplean como método de distribución un correo electrónico de phishing, que tiene adjunto un archivo como pdf o zip. En este aspecto, es necesario destacar los troyanos:

- **Mekotio**
- **Casbaneiro**
- **Amavaldo**
- **Grandoreiro**
- **Guilma**
- **Javalí**
- **Lampion**
- **Mispadu**
- **Bizarro**

En cuanto a los **RAT** o Remote Access Trojan, estos tuvieron **incremento en su uso** debido al aumento del uso de herramientas de acceso remoto por el **teletrabajo**. Algunos RAT han sido identificados en campañas dirigidas contra entidades financieras de Colombia:

- **NjRAT**
- **Remcos RAT**
- AsyncRAT, que podría corresponder a una nueva campaña de **APT-C-36**

El ransomware es un tipo de ciberamenaza que se ha caracterizado por:

- **Cambiar su modus operandi a doble extorsión** para exfiltrar información que es empleada para chantajear a las víctimas
- Incrementar su actividad
- Se destacan: **REvil, Maze, Lockbit, RagnarLocker, Sodinoki, DoppelPaymer, Nemty, Nefilim y CLOP**

Los ciberataques contra los dispositivos en el punto de venta o **POS** persisten, ya que es un malware que no requiere de una evolución ni adaptación según el dispositivo.

- En 2020 se han identificado **diversas campañas de RtPOS, MMON, PwnPOS y TinyPOS**

Las **APT** (Advanced Persistent Threat) con motivación financiera y de ciberespionaje han seguido muy presentes sobre las entidades del sector financiero. En 2020 se pueden destacar campañas de:

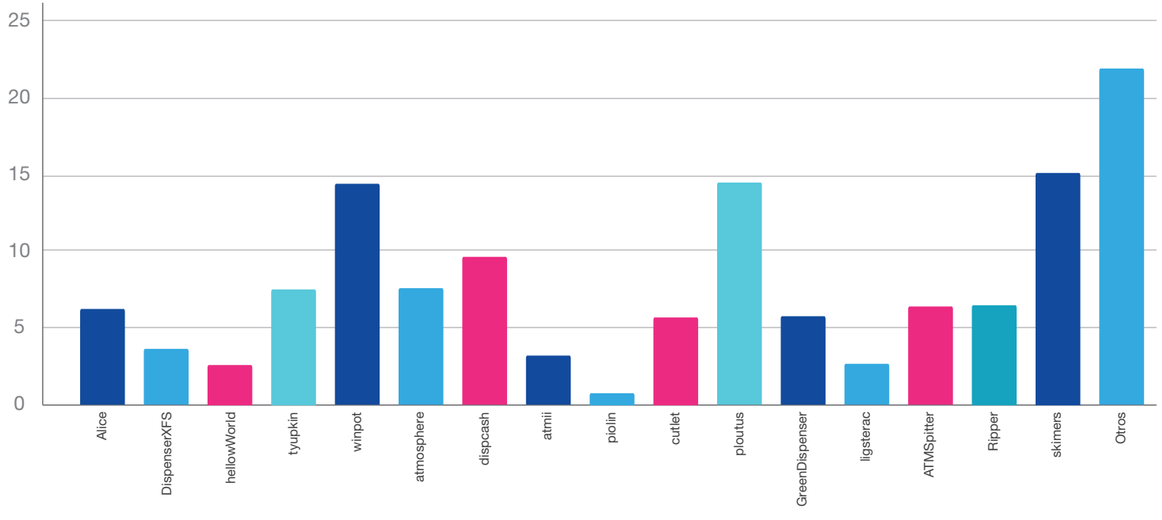
- **Grandes grupos: Lazarus, FIN7 o Silence**
- Nuevos grupos enmarcados en el Crime-as-a-Service (CaaS) como **DeathStalker**

Dentro de sus **capacidades sofisticadas** de ataque, se espera que las APT:

- Continúen explotando vulnerabilidades de software
- Empleen servicios legítimos en la nube para ocultar su infraestructura e incrementar su evasividad

Sobre los **ATM** y el uso de malware desarrollado para estos dispositivos, se ha visto en **descenso** durante 2020; sin embargo, el Csirt Financiero, ha llevado a cabo la **obtención y el análisis de más de 130 muestras** de malware, tal y como se muestra a continuación:

ATM Malware - Principales familias analizadas por el CSIRT Financiero



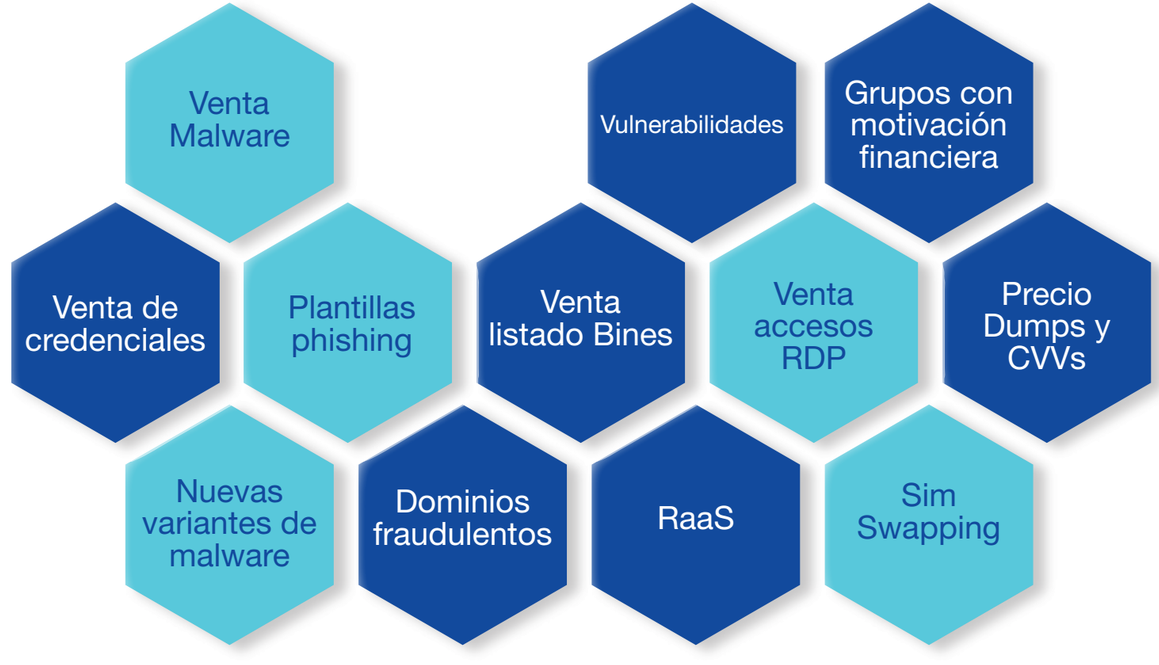
De los **hallazgos del Csirt Financiero** se destaca:

- La gran mayor parte de **muestras de ATM comparten código** entre variantes de la misma familia. Esto puede indicar, que los desarrolladores de malware ATM, son independientes y no comparten información entre los desarrolladores de cada familia.

Sobre la cuestión de los **dispositivos móviles,** durante 2020:

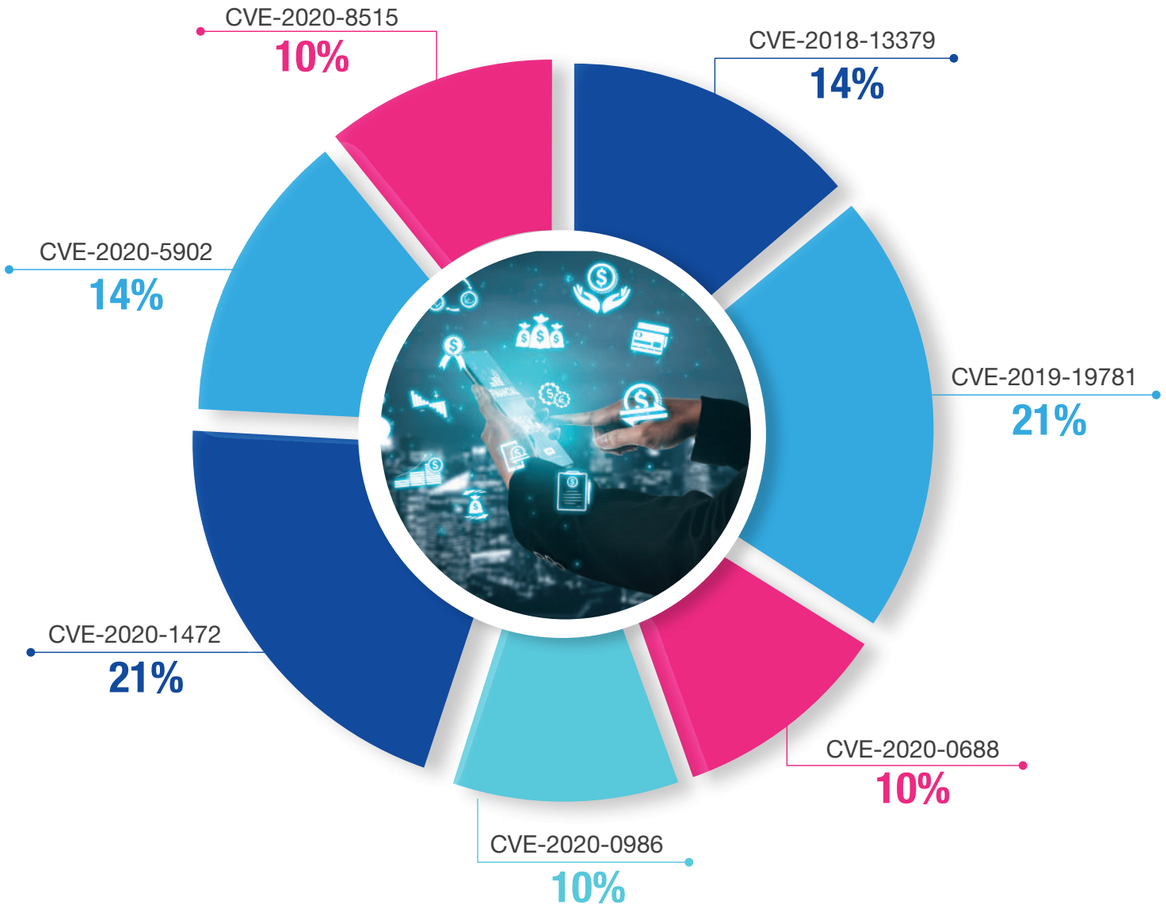
- Se **duplicó el volumen** de transacciones fraudulentas originadas desde aplicaciones móviles.
- Incremento de incidentes de **malware** contra estos dispositivos.
- Son, especialmente destacables, aquellos malware destinados a la **captación de datos confidenciales,** como credenciales bancarias.
- Se han identificado campañas con los malware **Cerberus, Alien y GINP.**
- En muchos casos se ha empleado la **técnica de superposición,** que ha incrementado su uso en 2020 y se espera su permanencia para 2021.

En último lugar, dentro del Observatorio de Ciberseguridad, se ha tratado la cuestión del **fraude y ciberamenazas identificadas en la Deep Web y Darknet.** Se ha detectado, a lo largo de 2020, un importante incremento de **campañas de phishing, estafas** y desarrollo del **CaaS**. Añadido a esto, se han identificado una multitud de productos vendidos en markets de la Deep Web y Darknet que pueden afectar, directa o indirectamente, a entidades del sector financiero. Las cuestiones tratadas se muestran a continuación:



Inteligencia de amenazas

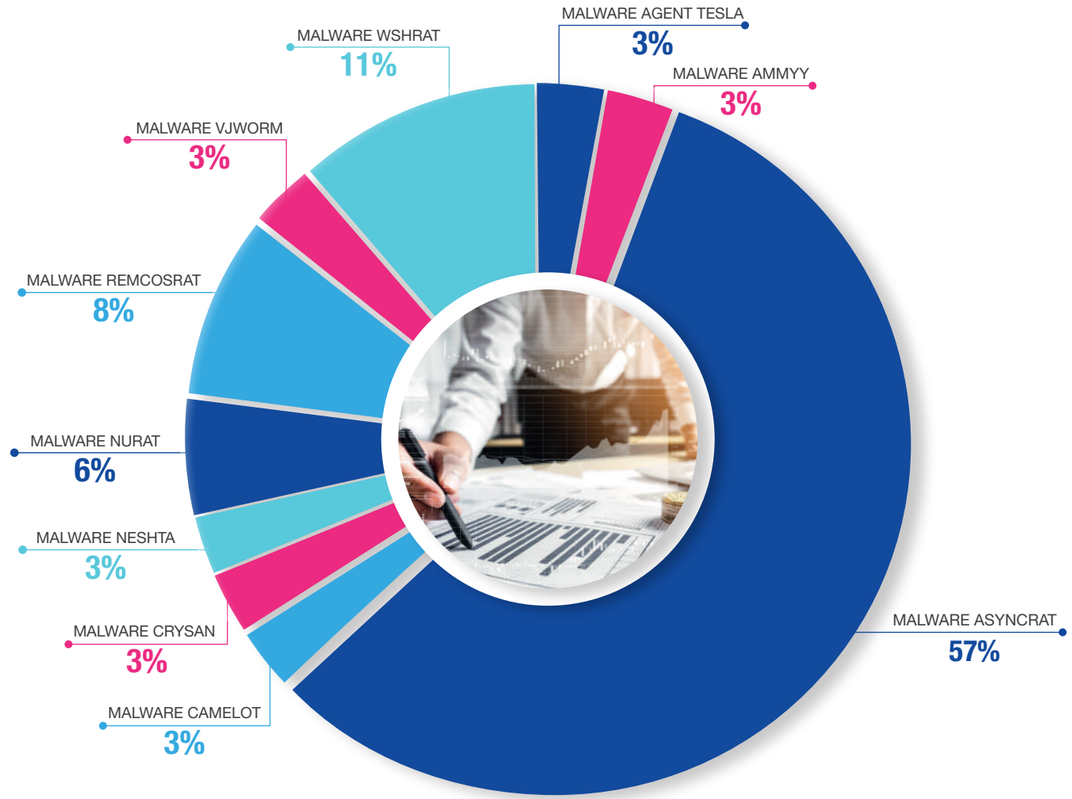
Top vulnerabilidades con mayor implicación en actividades maliciosas CSIRT



En el transcurso del 2020, el Csirt Financiero notificó **197 vulnerabilidades**, referidas en 12 alertas tempranas y 49 notificaciones. En el gráfico se muestran aquellas de **mayor impacto en las organizaciones** asociadas, con el objetivo de robar información y basadas en patrones, técnicas y brechas utilizadas por ciberdelincuentes.

Apoyo a incidentes

Como resultado de un trabajo colaborativo entre los asociados y el **Csirt Financiero**, se logró gestionar y brindar apoyo en **193 incidentes** que tienen relación con la distribución de sitios de phishing, suplantación de sitios web o phishing dirigido, análisis de malware e identificación de vulnerabilidades. A continuación, se muestran las familias de malware más reportadas en los incidentes:



Como medida de protección y prevención, el **Csirt Financiero** compartió con los asociados un total de **68** reglas de distintos fabricantes, que tiene como finalidad ser implementadas en **herramientas de seguridad tipo SIEM.**

Por último, y tras todos los análisis realizados por parte del equipo del Csirt Financiero, se brindan una serie de **tendencias identificadas** que marcarán el transcurso del **2021** y años próximos, todo con el fin de facilitar la prevención de futuras ciberamenazas.

Tendencias en Ciberseguridad

1. Ransomware como carga final y doble extorsión
2. Explotación de vulnerabilidades derivado de la situación de teletrabajo
3. Deep Fake e inteligencia artificial para hacer ataques personalizados y dirigidos
4. Vulnerabilidades de IoT que permiten recoger información durante el teletrabajo
5. Identidades sintéticas para realizar delitos como blanqueo de capital o servicio de mulas
6. Ataques más sofisticados y silenciosos por parte de los actores como las APT

Tendencias tecnológicas

1. Neobancos, digitalización de procesos, disminución de ATMs y dinero en efectivo
2. Tecnología Blockchain para una mayor inmediatez y trazabilidad de la transacción
3. Zero Trust para reducir el impacto de los incidentes de seguridad
4. BAS (Breach and Attack Simulation) para poner a prueba el nivel de seguridad y respuesta ante un ataque

ASOBANCARIA

Hernando José Gómez
Presidente

Mónica María Gómez Villafañe
Vicepresidente Administrativa y Financiera

Angela María Vaca
Directora Nuevos Negocios

MNEMO

Equipo técnico y de operación del CSIRT

Emanuel Ortiz
Codirector Operativo

Roberto Peña
Codirector Estrategia

Eva Moya
Responsable Implantación Estrategia

Jose Luis Sanchez
Director Técnico

Carlos Javier Beltrán
Coordinador Operación

Carlos Guzmán
Líder Técnico

Leticia Lanuza
Líder Dirección Documental

Carlos Rojas
Líder Gestión

Ximena Galindo
Líder Calidad

Belén Viqueira
Tendencias y Prospectiva

MOUSE GRAPHIC

Adriana Cuéllar González
Diseño y Diagramación

CSIRT FINANCIERO

www.csirtasobancaria.com
csirt@asobancaria.com
incidente@csirtasobancaria.com
Tel: (+571) 4391639
018000111505
+57 3174345665

@CSIRTFinanciero

ASOBANCARIA

Construyendo
la **Confianza** y **Solidez** del sector financiero