Informe de apreciación Sector Financiero

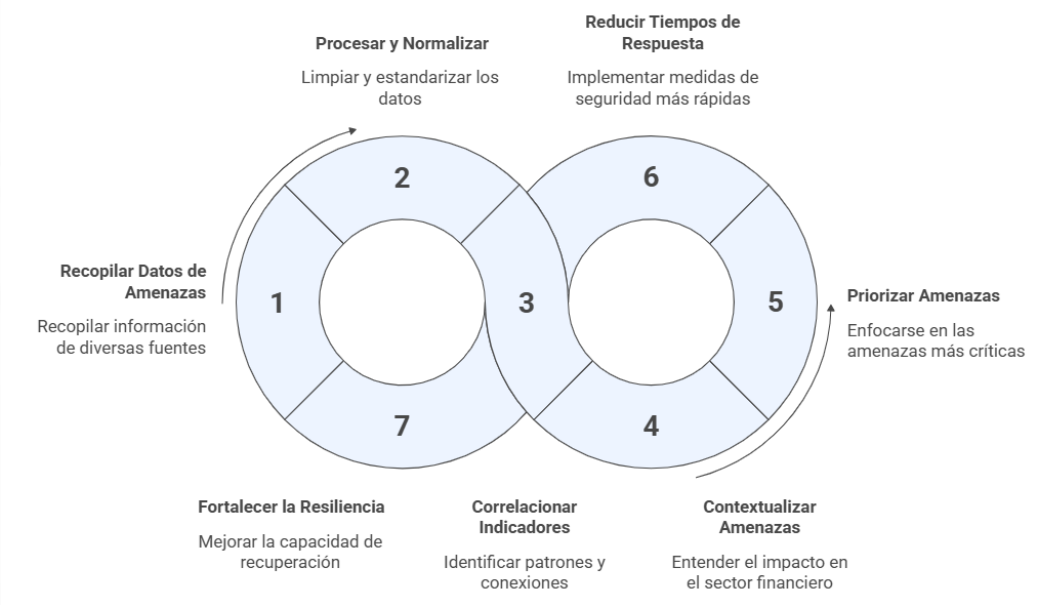
COLCERT

Contenido

INTRODUCCIÓN

En el sector financiero colombiano, la acelerada digitalización de los servicios y la adopción de sistemas de pagos inmediatos han expandido significativamente la superficie de exposición a ciberamenazas. Actores de amenazas avanzadas (APT), grupos de cibercrimen organizado y operadores de ransomware dirigen sus esfuerzos hacia las entidades del sector, buscando comprometer la integridad de los activos, la confidencialidad de los datos y la continuidad de los servicios financieros esenciales.

Este informe emplea inteligencia de amenazas para realizar un seguimiento riguroso al comportamiento de los actores que afectan el ecosistema financiero nacional, fundamentado en la consolidación de información técnica reciente. Se priorizan fuentes de visibilidad estratégica que permiten identificar amenazas relevantes para la estabilidad económica y la infraestructura crítica del país.



Lineamientos

- Seguimiento a actores que afectan el sector financiero colombiano.
- Uso de inteligencia de amenazas para la toma de decisiones estratégicas.
- Priorización de fuentes de ciberinteligencia aplicables al contexto nacional.
- Enfoque en la protección de infraestructuras críticas financieras.
- Reducción de tiempos de detección y respuesta ante incidentes de fraude o intrusión.
- Fortalecimiento de la resiliencia cibernética y la confianza sistémica del sector.

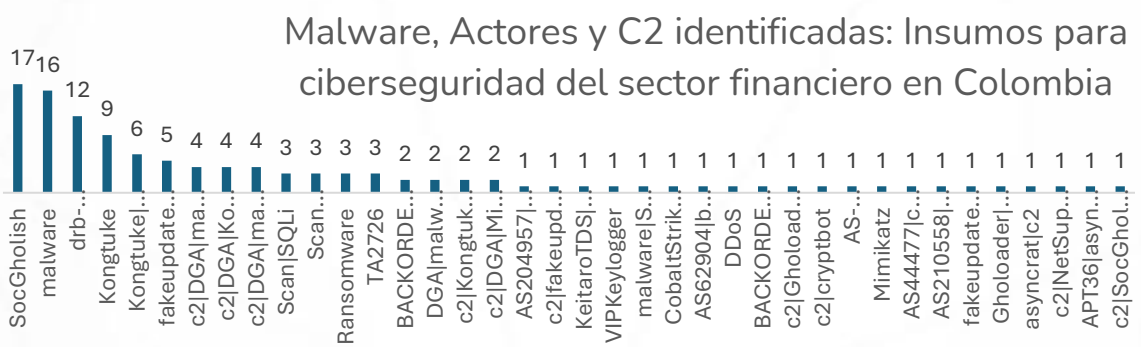
RESUMEN EJECUTIVO

El presente informe ofrece un análisis estratégico del panorama de amenazas cibernéticas dirigido al sector financiero colombiano con corte a mayo de 2026. A través de la evaluación de actores de amenazas avanzadas y el procesamiento de 3,812 indicadores de compromiso, donde se identifican los vectores de ataque y patrones de infraestructura que representan el mayor riesgo para la estabilidad y la confianza del sistema bancario nacional.

Aspectos clave:

- Diversificación del arsenal de ataque.
- Volumen de exposición digital.
- Enfoque geográfico específico en Colombia.

Hallazgos Clave



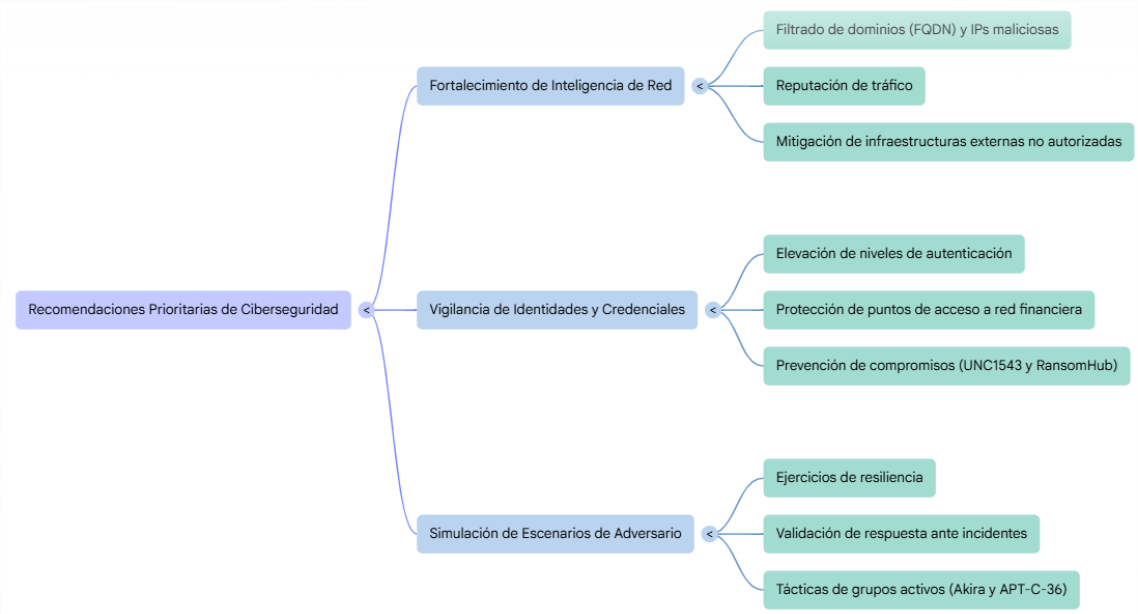
- **Persistencia de Actores Especializados:** Se identifica una actividad crítica de grupos de amenazas avanzadas (APTs) que históricamente han dirigido sus operaciones hacia la infraestructura financiera. Grupos como FIN7 (especializado en fraude financiero) y Blind Eagle (con un enfoque persistente en Colombia) lideran el volumen de actividad detectada.

- **Diversificación del Arsenal de Ataque:** La presencia de actores como APT44 y APT34 sugiere un interés que trasciende el robo directo de activos, enfocándose en el espionaje corporativo y la interrupción de servicios críticos.

- **Volumen de Exposición Digital:** Se ha registrado un inventario de 3,812 indicadores de compromiso, donde la infraestructura de red (dominios y direcciones IP) representa más del 86% de los activos utilizados por los adversarios para el despliegue de sus campañas.

- **Enfoque Geográfico Específico:** Una proporción significativa de los adversarios activos tiene operaciones rastreadas específicamente bajo la denominación COLOMBIA, lo que confirma que el país es un objetivo táctico y no solo colateral en las campañas globales.

Recomendaciones Prioritarias

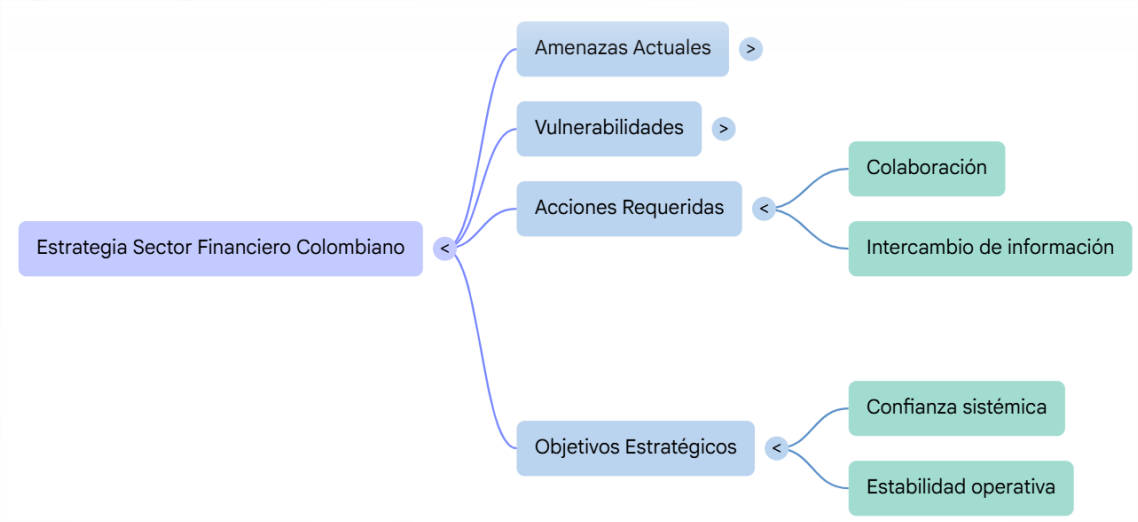


- **Fortalecimiento de la Inteligencia de Red:** Dada la alta prevalencia de dominios (FQDN) y direcciones IP maliciosas, es imperativo reforzar las políticas de filtrado y reputación de tráfico para mitigar comunicaciones con infraestructuras externas no autorizadas.

- **Vigilancia de Identidades y Credenciales:** Los actores identificados (como UNC1543 y RansomHub) suelen utilizar el acceso inicial basado en el compromiso de identidades; se recomienda elevar los niveles de autenticación en todos los puntos de acceso a la red financiera.

- **Simulación de Escenarios de Adversario:** Ejecutar ejercicios de resiliencia basados en las tácticas de los grupos con mayor actividad reciente (ej. Akira y APT-C-36) para validar la capacidad de respuesta ante incidentes de alto impacto.

Conclusión Estratégica

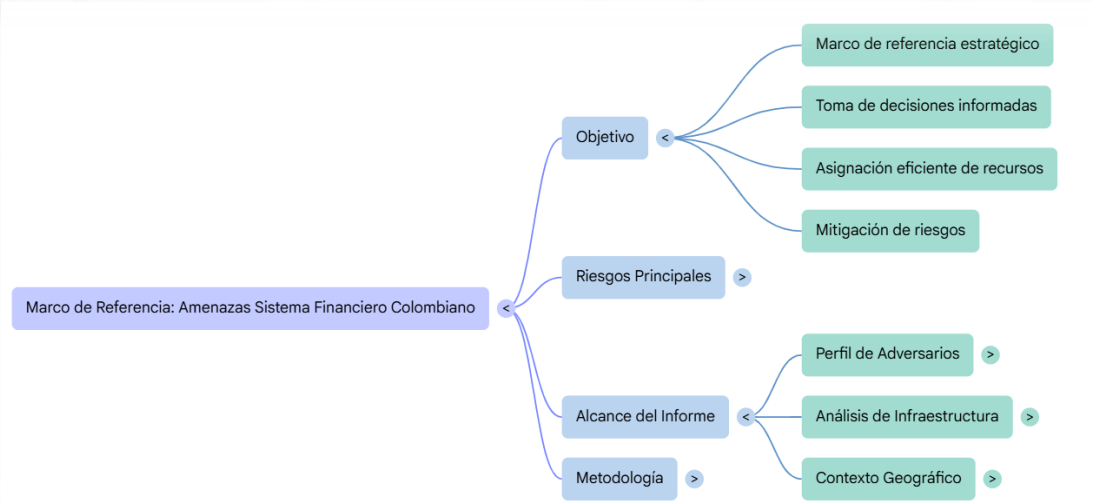


El sector financiero colombiano se encuentra bajo un estado de observación constante por parte de grupos criminales con alta capacidad técnica. La transición hacia servicios digitales y pagos inmediatos ha expandido la superficie de ataque, haciendo que la colaboración y el intercambio de información sobre amenazas sea la única vía para mantener la confianza sistémica y la estabilidad operativa del sector.

Puntos Clave:

- Estado de observación constante por grupos de alta capacidad técnica.
- Expansión de la superficie de ataque por servicios digitales y pagos inmediatos.
- Necesidad de colaboración e intercambio de información sistémica.
- Prioridad en mantener la estabilidad operativa y la confianza del sector.

OBJETIVO Y ALCANCE



Objetivo

Establecer un marco de referencia estratégico sobre las amenazas más relevantes que impactan al sistema financiero colombiano. El propósito es facilitar la toma de decisiones informadas por parte de los directivos, permitiendo la asignación eficiente de recursos para la mitigación de riesgos de fraude, espionaje y afectación de la disponibilidad del servicio.

Alcance

El alcance de este informe se centra en la identificación y caracterización de los principales grupos de amenazas que dirigen sus operaciones hacia el territorio nacional, analizando sus patrones de infraestructura y vectores de ataque específicos para las instituciones reguladas. A través de un enfoque basado en datos técnicos actuales, se delimita el espectro de exposición del ecosistema financiero colombiano frente a tácticas de espionaje, fraude y sabotaje digital.

Este informe comprende el análisis de:

- ✓ Perfil de los Adversarios: Evaluación de 15 grupos de amenazas con actividad reciente o histórica dirigida contra Colombia y sus instituciones financieras.
- ✓ Análisis de Infraestructura: Desglose de los medios técnicos (identificadores de red y archivos) utilizados por estos grupos, basados en un conjunto de 3,812 elementos de análisis recolectados de fuentes de inteligencia hasta mayo de 2026.

- ✓ Contexto Geográfico: Enfoque exclusivo en la actividad que tiene incidencia directa en el territorio nacional y en entidades que operan bajo la regulación financiera colombiana.

Definición y Entendimiento del Sector

El sector financiero en Colombia se constituye como el pilar de la estabilidad económica nacional, integrando establecimientos de crédito, sociedades de servicios financieros y entidades de regímenes especiales bajo un marco regulatorio estricto. En la actualidad, este ecosistema atraviesa una fase de convergencia entre la banca tradicional y modelos de finanzas abiertas (Open Banking), lo que incrementa la interdependencia entre instituciones y la necesidad de una defensa coordinada frente a amenazas que puedan comprometer la confianza sistémica.

- Pilar de estabilidad económica nacional.
- Convergencia entre banca tradicional y finanzas abiertas.
- Marco regulatorio estricto y supervisado.
- Alta interdependencia operativa entre instituciones.
- Necesidad de defensa coordinada y sistémica.

Superficie de Ataque

La superficie de ataque del sector financiero colombiano se ha expandido más allá de los perímetros tradicionales debido a la adopción masiva de canales digitales, plataformas de pagos inmediatos y el uso de infraestructuras en la nube. Esta exposición se ve reflejada en un inventario crítico de activos digitales que los adversarios explotan para establecer persistencia, destacando una alta prevalencia de infraestructuras de red y puntos de acceso remoto como los principales vectores de incursión.

- Adopción masiva de canales digitales y pagos inmediatos.
- Uso extensivo de infraestructuras en la nube.
- Exposición de perímetros más allá de la banca tradicional.
- Predominancia de activos de red (FQDN e IPs) como vectores de riesgo.
- Vulnerabilidad en puntos de acceso remoto y gestión de identidades.

PANORAMA ACTUAL DE AMENAZAS

El panorama actual de amenazas para el sector financiero colombiano durante el primer cuatrimestre de 2026 se caracteriza por una alta frecuencia de incidentes que impactan tanto la disponibilidad de los servicios como la integridad de la información

confidencial. La siguiente recopilación de eventos críticos evidencia una tendencia creciente en delitos informáticos y brechas de datos a gran escala, subrayando la vulnerabilidad de las cadenas de suministro y la necesidad de robustecer los canales digitales ante fallas operativas y ataques dirigidos que afectan a millones de usuarios en el país.

TÍTULO	FECHA	FUENTE
Organizaciones enfrentan 2.803 ataques cibernéticos semanales	24/04/2026	La Republica
Caída de Bancolombia: falla global afecta millones	25/02/2026	Cronista.com
Bancolombia se pronunció sobre crisis en canales digitales	25/02/2026	Infoabe
Delitos informáticos rompen récord en Colombia	18/03/2026	Infoabe
Bancolombia responde a fallas en app (más de 12 horas)	22/02/2026	Caracol

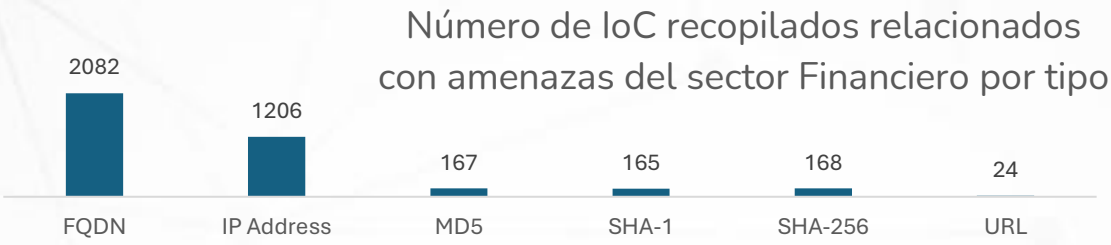
Tipología de Eventos Identificados

El análisis de los indicadores técnicos permite clasificar las amenazas según su naturaleza y nivel de impacto potencial sobre la infraestructura financiera nacional. Esta categorización facilita la comprensión de cómo los adversarios despliegan sus recursos, desde la suplantación de identidades mediante dominios fraudulentos hasta la ejecución de software malicioso diseñado para el robo de activos. La identificación de estas tipologías es fundamental para priorizar los esfuerzos de defensa y anticipar las tácticas de grupos especializados que operan activamente contra las entidades del país.

Tipo de IoC	Volumen estimado	Fuentes principales	Relevancia por sector financiero
Dominios (FQDN)	Alto (más de 500 registros activos)	Google Threat Intelligence, MISP Import	**Crítica.** Dominios que suplantan servicios legítimos evidencian campañas de phishing para robar credenciales de banca en línea y acceso a sistemas financieros. La presencia de infraestructura de Comando y Control (C2) activa sugiere intentos de persistencia en las redes.
Direcciones IP	Muy alto (miles de registros activos)	Google Threat Intelligence, MISP Import	**Crítica.** Representan infraestructura de comando, servidores de phishing o proxies maliciosos apuntando a entidades colombianas. La alta concentración de IPs activas desde abril de 2026 indica una amenaza persistente y actualizada para el sector.
Hashes (MD5, SHA-g1, SHA-256)	Muy alto (miles de registros activos)	Google Threat Intelligence, MISP Import, Malpedia, AlienVault OTX Pulse	**Alta.** Asociados a malware bancario, troyanos de acceso remoto (RAT), stealers y ransomware (Akira, RansomHub). Actores como FIN7, APT34 y Blind Eagle utilizan estos elementos para comprometer la integridad de las operaciones financieras.
URLs	Moderado (muestra representativa)	Google Threat Intelligence	**Alta.** Sugieren intentos de descarga de configuraciones maliciosas o payloads. Se utilizan para alojar archivos de configuración de malware bancario, scripts de recolección de credenciales o páginas de phishing que simulan entidades financieras legítimas.

Fuente: https://www.datos.gov.co/stories/s/rgem-8mys

INDICADORES DE COMPROMISO (IoCs)



Esta sección detalla los elementos técnicos que permiten identificar y rastrear actividades maliciosas dirigidas contra el ecosistema financiero del país. Los Indicadores de Compromiso (IoCs) recopilados representan la evidencia digital de la infraestructura utilizada por los adversarios, desde nombres de dominio fraudulentos hasta huellas digitales de software malicioso. El análisis cuantitativo de estos datos revela una marcada concentración en activos de red, lo que subraya la importancia de fortalecer las capacidades de detección temprana y bloqueo preventivo para mitigar posibles intrusiones o fraudes financieros.

Resumen de IoCs Relevantes

Esta sección presenta una selección estratégica de los indicadores que, por su nivel de criticidad y actividad reciente, representan la amenaza más directa para las entidades del sector financiero colombiano. Se destacan activos de red y firmas de archivos asociados a campañas de suplantación de identidad (phishing), infraestructuras de Comando y Control (C2) y despliegue de software malicioso especializado en el robo de activos bancarios. El monitoreo prioritario de estos elementos es esencial para prevenir brechas de seguridad y mitigar el impacto operativo en las instituciones financieras.

Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Adversarios Detectados	Identificación de 15 grupos (APTs y financieros como FIN7 y Blind Eagle) con operaciones activas contra la infraestructura nacional.	Crítico
Infraestructura C2	Predominancia de dominios y direcciones IP (más de 3,200 registros) configurados para el comando y control de activos del sector.	Muy Alto
Familias de Malware	Presencia de agentes especializados como malware bancario, troyanos de acceso remoto y ransomware (Akira, RansomHub).	Alto
Vectores de Incursión	Uso de campañas de phishing mediante suplantación de servicios corporativos (Microsoft, Office 365) para el robo de credenciales.	Muy Alto
Severidad de Alertas	Concentración masiva de indicadores de red con puntuaciones de riesgo (Score) críticas, alcanzando niveles de 11/15 y 14/15.	Crítico

Aspectos clave evidenciados:

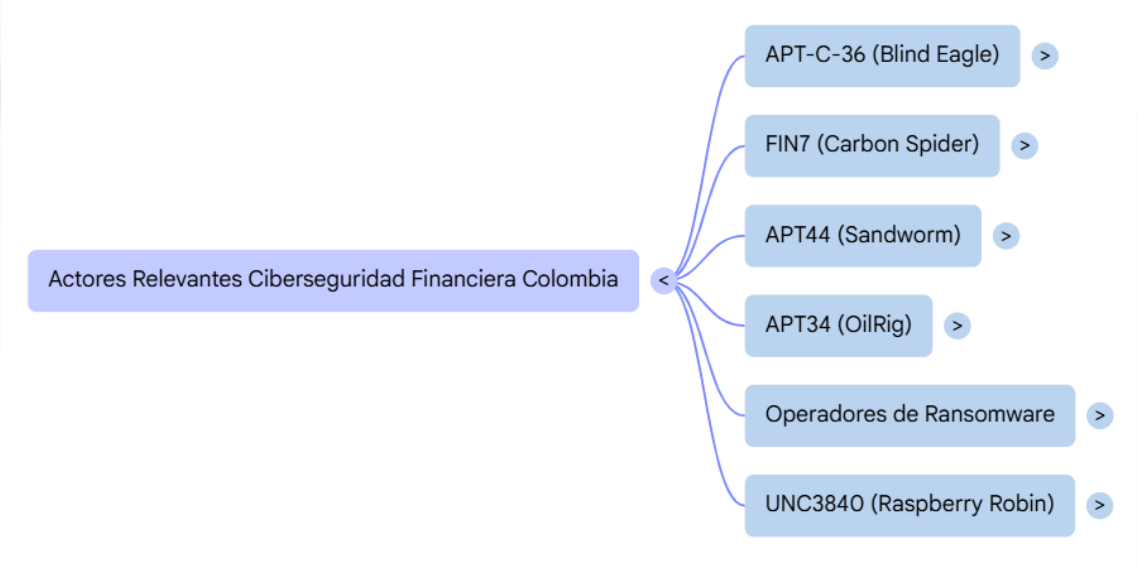
- Persistencia de actores especializados (FIN7, Blind Eagle).
- Diversificación del arsenal de ataque (APTs y Ransomware).
- Volumen crítico de exposición digital (3,812 indicadores).
- Enfoque geográfico específico en Colombia.
- Predominancia de infraestructura de red (dominios e IPs).
- Suplantación de servicios corporativos y financieros.
- Alta severidad de alertas con puntuaciones de riesgo críticas.

ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

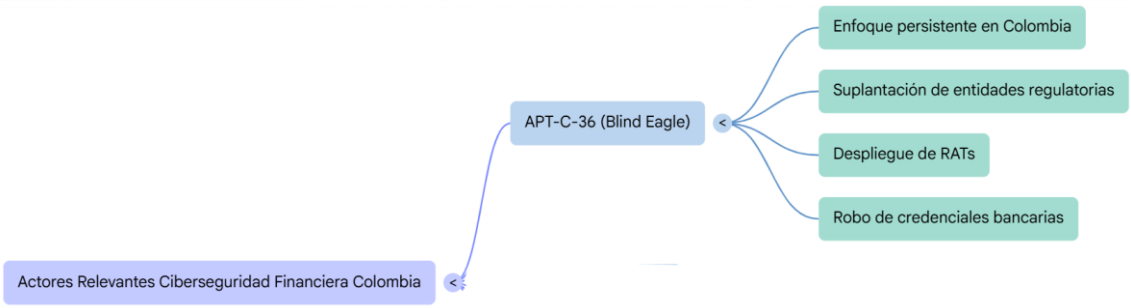
Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Grupos de Ciber-Crimen Financiero	5	FIN7, Carbanak, Carbon Spider, Sangria Tempest, TelePort Crew.	*Extremo.* Especializados en el despliegue de malware bancario, robo de datos de tarjetas y fraude transaccional a gran escala.
Amenazas Avanzadas Persistentes (APT)	6	APT44 (Sandworm), APT34 (OilRig), APT19, APT-C-36 (Blind Eagle), UNC1543, UNC2505.	*Crítico.* Enfocados en el espionaje corporativo y la infiltración de infraestructuras críticas para el robo de información estratégica.
Operadores de Ransomware	2	Akira, RansomHub.	*Muy Alto.* Representan la principal amenaza para la disponibilidad operativa, mediante el cifrado de datos y la extorsión por exfiltración.
Actores de Intrusión y Acceso Inicial	2	UNC3840 (Raspberry Robin), UNC5537.	*Alto.* Actúan como facilitadores para otros grupos, estableciendo persistencia inicial en las redes para la posterior entrega de cargas útiles.

Identificación de Actores Relevantes

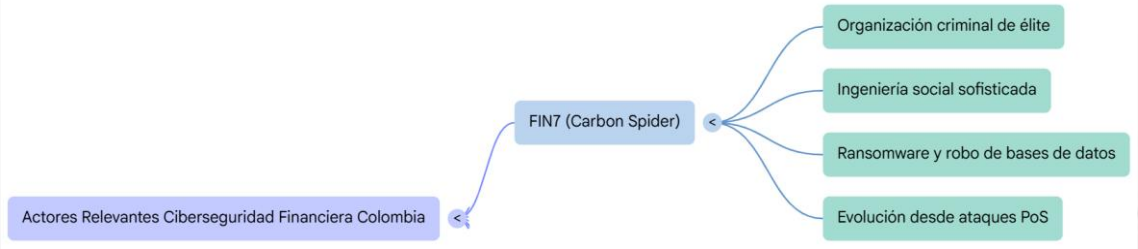
El análisis ha permitido identificar 15 adversarios con distintos niveles de actividad para el sector financiero colombiano. Entre ellos, tres actores destacan con actividad en Colombia y reconocido historial de ataques al sector financiero global: FIN7, APT34 y APT44, todos actualizados en junio de 2026.



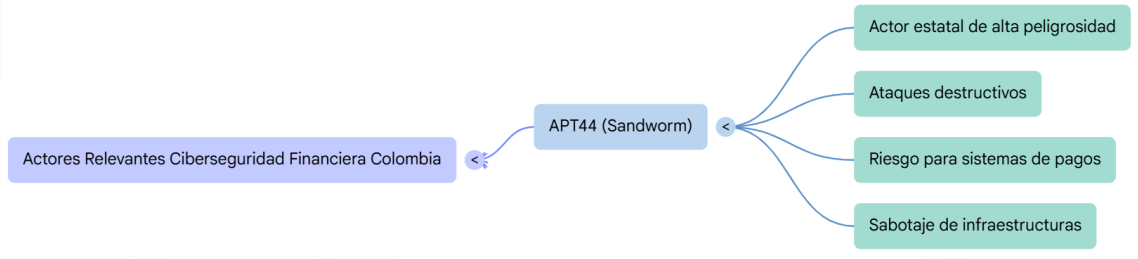
APT-C-36 (Blind Eagle): Actor de ciberespionaje con un enfoque desproporcionado y persistente en Colombia. Se especializa en la suplantación de entidades regulatorias y judiciales nacionales para desplegar troyanos de acceso remoto (RATs), facilitando el robo de credenciales bancarias y la exfiltración de datos financieros sensibles.



FIN7 (Carbon Spider): Organización criminal de élite con vasta experiencia en intrusiones a instituciones financieras. Han evolucionado de ataques a terminales de punto de venta (PoS) hacia operaciones complejas de ransomware y robo de bases de datos, utilizando técnicas de ingeniería social altamente sofisticadas dirigidas a empleados bancarios.



APT44 (Sandworm): Actor estatal de altísima peligrosidad. Aunque su origen es el sabotaje de infraestructuras energéticas, su capacidad para ejecutar ataques destructivos representa un riesgo extremo para la disponibilidad de los sistemas de liquidación y compensación de pagos en tiempo real.

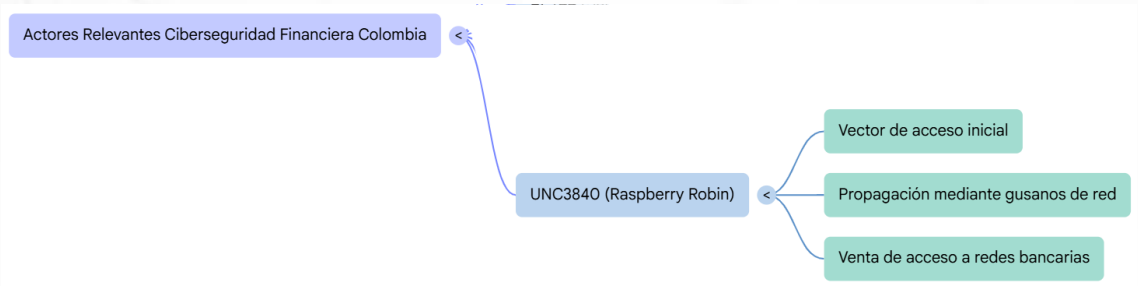


APT34 (OilRig): Grupo especializado en ciberespionaje de largo aliento. Su interés en el sector financiero radica en el reconocimiento de redes estratégicas y la interceptación de comunicaciones corporativas para obtener ventajas competitivas o políticas a través de la infiltración de servidores de correo y bases de datos.

RansomHub y Akira: Operadores de ransomware que ejecutan modelos de doble extorsión. Su presencia en los indicadores recopilados sugiere un interés activo en paralizar la continuidad operativa de las entidades financieras, amenazando con filtrar información confidencial de clientes si no se cumplen sus demandas económicas.

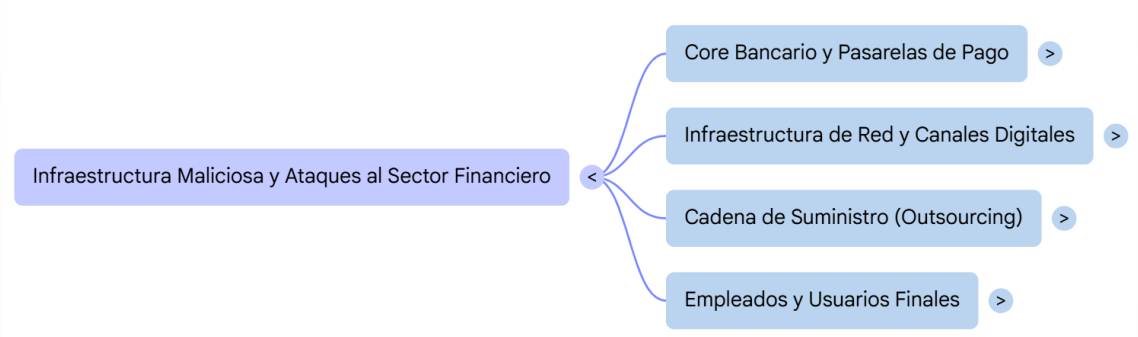
UNC3840 (Raspberry Robin): Un sofisticado vector de acceso inicial que utiliza gusanos de red para propagarse. Actúa como el primer eslabón en la cadena de ataque,

permitiendo que otros actores financieros de mayor nivel (como operadores de ransomware) compren el acceso a redes bancarias ya comprometidas.



Objetivos y Sectores Target

El análisis de la infraestructura maliciosa detectada confirma que el sector financiero es el objetivo principal de estas operaciones, con una estrategia de ataque que se ramifica hacia sectores interconectados para maximizar el impacto sistémico.



- **Core Bancario y Pasarelas de Pago:** Ataques dirigidos a comprometer la integridad de las transacciones y la disponibilidad de los servicios de banca en línea.

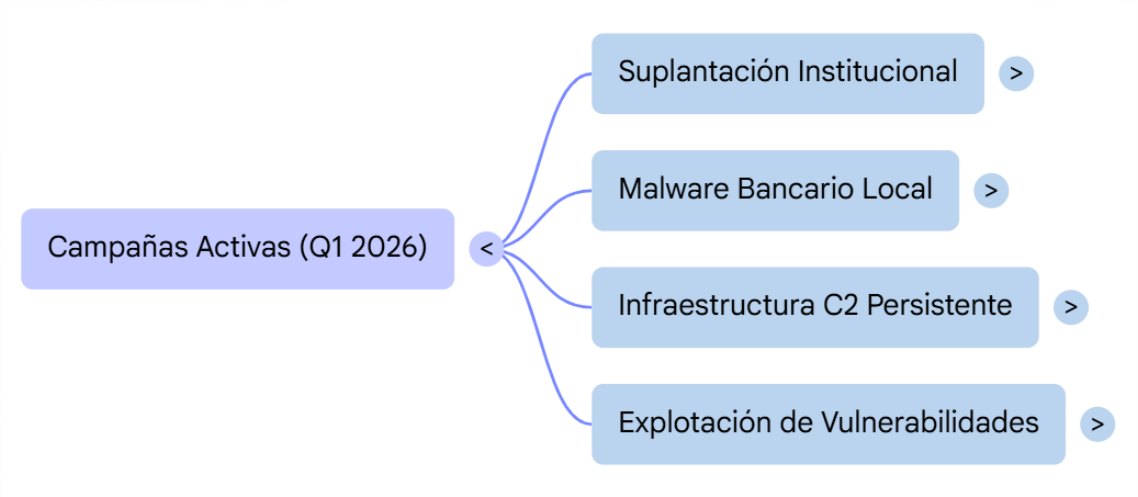
- **Infraestructura de Red y Canales Digitales:** Debido a la expansión de la superficie de ataque, los adversarios priorizan la explotación de activos de red, puntos de acceso remoto y servicios en la nube.

- **Cadena de Suministro (Outsourcing):** Se evidencia un creciente interés en proveedores críticos de servicios tecnológicos (BPO, servicios de nube) como vector indirecto para alcanzar a las entidades financieras reguladas.

- **Empleados y Usuarios Finales:** Siguen siendo el eslabón de acceso inicial mediante campañas masivas de phishing que suplantan identidades corporativas de alto perfil.

Campañas Activas

Durante el primer cuatrimestre de 2026, se han documentado campañas específicas que utilizan infraestructura técnica de alta severidad para evadir controles tradicionales.



- **Campaña de Suplantación Institucional:** Uso de dominios como microsoft-um.xyz y office365-management.com con el fin de recolectar credenciales de acceso de funcionarios bancarios.
- **Despliegue de Malware Bancario Local:** Distribución activa de variantes de troyanos adaptados al lenguaje y contexto colombiano, facilitando el control remoto de estaciones de trabajo y el robo de sesiones activas.
- **Infraestructura C2 Persistente:** Se mantiene una red de Comando y Control (C2) con más de 3,200 indicadores activos, diseñada para establecer persistencia prolongada dentro de las redes financieras sin ser detectada.
- **Explotación de Vulnerabilidades en Servicios Expuestos:** Campañas dirigidas a la identificación de configuraciones débiles en servidores y aplicaciones web, evidenciadas por la detección de URLs de descarga de payloads maliciosos.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

A partir de la evidencia recolectada y correlacionada por el equipo de CTI —incluyendo IOCs de phishing, hashes de malware, IPs de C2, dominios DGA y etiquetas como Scan Network, SQLi, Ransomware y DDoS—, se han identificado las siguientes tácticas y técnicas del marco MITRE ATT&CK que aplican a las cadenas de ataque observadas contra el sector financiero Colombia.

Identificación	Nombre en inglés	Justificación en español
TA0043	Reconocimiento	Los actores FIN7 y APT34 realizan reconocimiento activo de dominios de entidades financieras colombianas, como lo evidencian los FQDNs fraudulentos asociados y los escaneos previos a campañas de phishing..
TA0001	Acceso inicial	El acceso inicial se ha observado mediante campañas de phishing con dominios fraudulentos (microsoft-um.xyz, adobeprotect.com) y documentos maliciosos que, al ser ejecutados por usuarios del sector financiero, descargan malware.
TA0002	Ejecución	Los hashes de malware con score 11 identificados en ThreatQ corresponden a ejecutables que, una vez descargados, utilizan intérpretes de comandos y scripts para desplegar cargas maliciosas en equipos de entidades financieas..
TA0003	Persistencia	Los adversarios establecen persistencia mediante técnicas de programación de tareas (Scheduled Tasks) y modificación del registro, asegurando que el malware bancario o RAT permanezca activo tras reinicios del sistema.
TA0005	Evasión de defensa	Los indicadores muestran el uso de ofuscación de archivos (hashes maliciosos con nombres genéricos), ejecución de binarios del sistema para evadir detección y cifrado de comunicaciones con servidores C2..
TA0006	Acceso con credenciales	Actores como APT34 y Blind Eagle emplean técnicas de captura de credenciales mediante keylogging, dumping de procesos LSASS y phishing de credenciales de banca en línea a través de formularios falsos.
TA0008	Movimiento lateral	Una vez dentro de una entidad financiera, los adversarios utilizan servicios remotos (RDP, SMB) y cuentas válidas comprometidas para moverse hacia servidores de base de datos y sistemas transaccionales.
TA0011	Mando y control	Las IPs con score 14 (109.70.100.1, 87.118.122.30) y los FQDNs con score 11 (uz3.me, lh1v.club) representan servidores C2 que utilizan protocolos de capa de aplicación para mantener comunicación con malware desplegado.
TA0040	Impacto	Los actores Akira y RansomHub, presentes en ThreatQ, aplican técnicas de impacto mediante el cifrado de datos (ransomware), destrucción de información y detención de servicios críticos como plataformas de pagos y banca en línea.

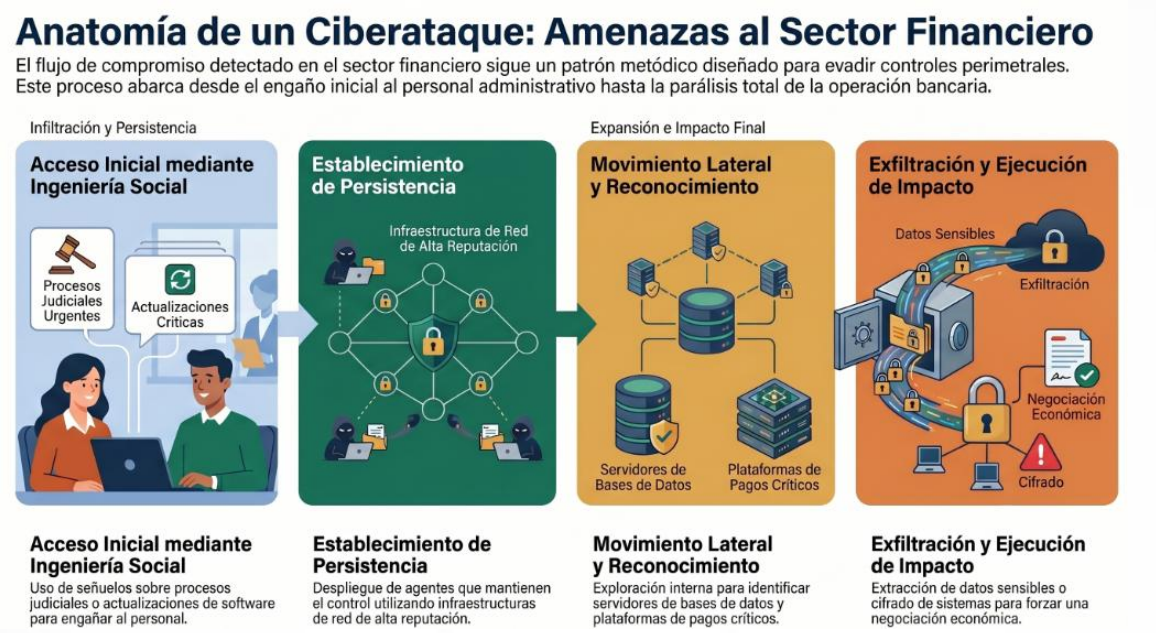
Identificación	Nombre en inglés	Justificación en español
T1566	Suplantación de identidad	Los dominios fraudulentos microsoft-um.xyz, office365-management.com, adobeprotect.com y firefox-uk.xyz evidencian campañas activas de phishing dirigidas a empleados del sector financiero para robar credenciales..
T1059	Intérprete de comandos y scripts	Los hashes de malware con score 11 están asociados a scripts maliciosos (PowerShell, VBScript) que descargan payloads adicionales o ejecutan comandos en sistemas bancarios comprometidos.
T1071	Protocolo de capa de aplicación	Las IPs de C2 con score 14 (109.70.100.1, 87.118.122.30) y los FQDNs uz3.me y lh1v.club utilizan protocolos HTTP/S y DNS para comunicarse con malware desplegado en entidades financieras.
T1003	Extracción de credenciales del sistema operativo}	Actores como FIN7 y APT34 son conocidos por volcar credenciales del archivo LSASS en sistemas comprometidos para acceder a cuentas de administradores de redes bancarias.
T1105	Transferencia de herramientas de Ingress	Los IOC de tipo URL (94.185.85.122/public/config.bak) y la presencia de hashes de malware indican la transferencia de herramientas maliciosas desde servidores C2 a equipos del sector financiero.
T1027	Archivos o información ofuscada	Los hashes de malware con nombres ofuscados y la presencia de archivos codificados (ej. archivos .bak sospechosos) evidencian técnicas de ofuscación para evadir antivirus y EDR.
T1078	Cuentas válidas	El etiquetado de actores como APT44 y FIN7, junto con las IPs de C2, sugiere el uso de cuentas de usuario válidas previamente comprometidas para acceder a sistemas financieros de manera legítima.
T1048	Exfiltración mediante protocolo alternativo	Las IPs de C2 y los FQDNs con score alto indican que la exfiltración de datos bancarios robados (credenciales, información de cuentas) podría realizarse por protocolos alternativos como FTP o WebDAV.
T1486	Datos cifrados para mayor impacto	La presencia de los adversarios Akira y RansomHub en ThreatQ, ambos asociados a ransomware, confirma la aplicación de técnicas de cifrado de datos para extorsionar a entidades financieras.
T1090	Apoderado	Las IPs maliciosas identificadas (ej. 23.191.200.28) pueden estar actuando como proxies para redirigir el tráfico de C2 y ocultar la ubicación real de los servidores de ataque contra el sector.

Cadenas de Ataque Observadas

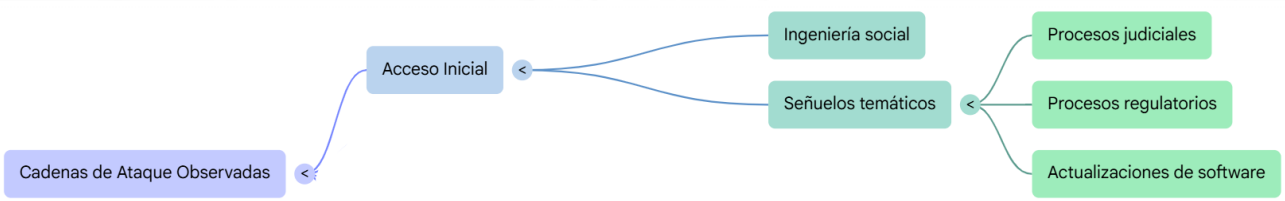
Para las secciones finales del análisis operativo, se presentan las dinámicas de intrusión y el arsenal digital identificado, estructurado bajo un enfoque estratégico para el sector financiero colombiano:

Cadenas de Ataque:

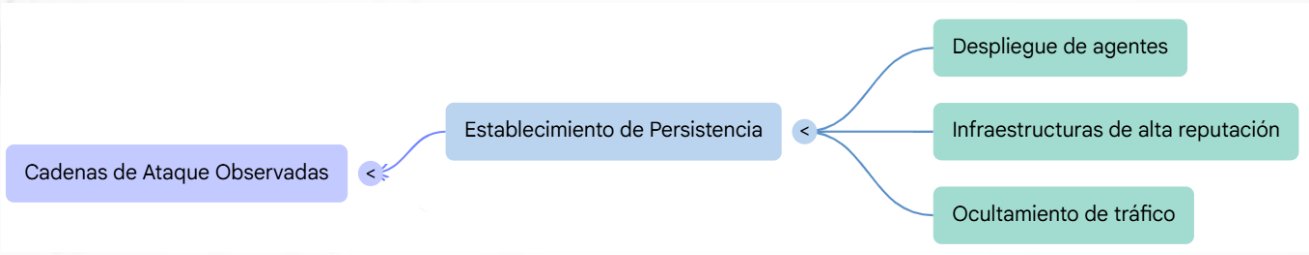
El flujo de compromiso detectado sigue un patrón metódico diseñado para evadir los controles perimetrales de las instituciones financieras. La cadena de ataque se desglosa en las siguientes fases operativas:



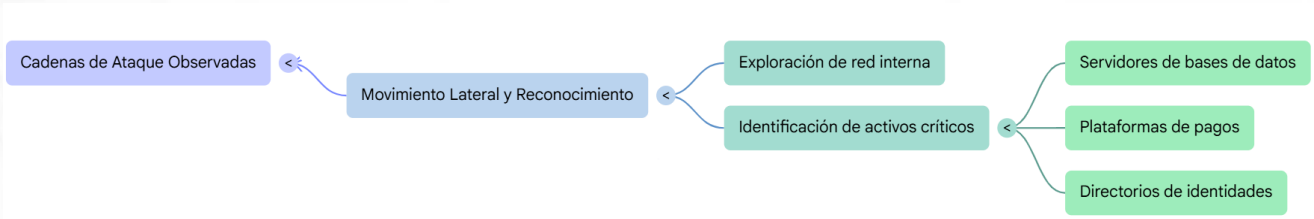
- **Acceso Inicial:** Se prioriza la ingeniería social mediante el uso de señuelos temáticos relacionados con procesos judiciales, regulatorios o actualizaciones de seguridad de software corporativo para engañar al personal administrativo.



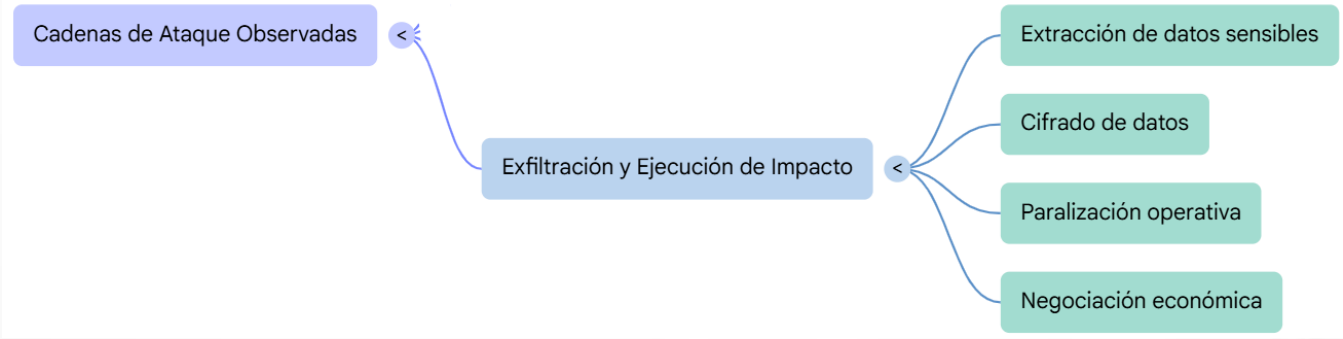
- **Establecimiento de Persistencia:** Una vez ejecutado el acceso inicial, los atacantes despliegan agentes que permiten mantener el control del equipo comprometido incluso tras reinicios del sistema, utilizando infraestructuras de red de alta reputación para ocultar el tráfico.



- **Movimiento Lateral y Reconocimiento:** Los adversarios exploran la red interna buscando identificar activos críticos como servidores de bases de datos, plataformas de pagos y directorios de gestión de identidades.



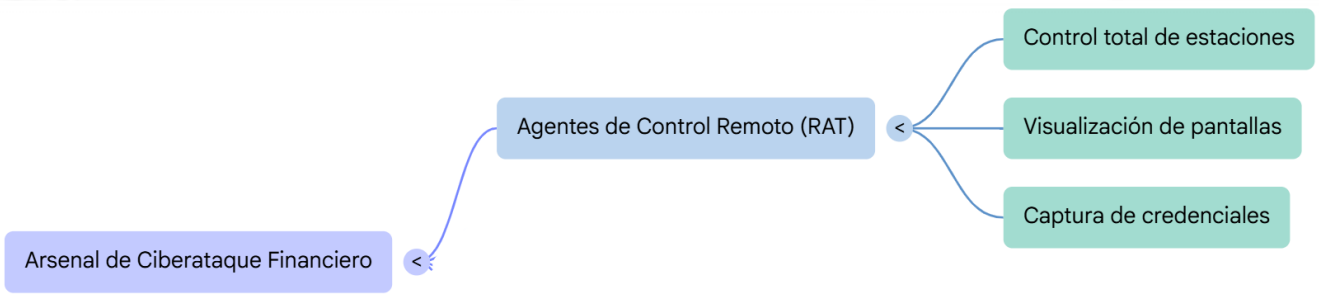
- **Exfiltración y Ejecución de Impacto:** La fase final consiste en la extracción de datos sensibles de clientes o la ejecución de software de cifrado para paralizar la operación bancaria y forzar una negociación económica.



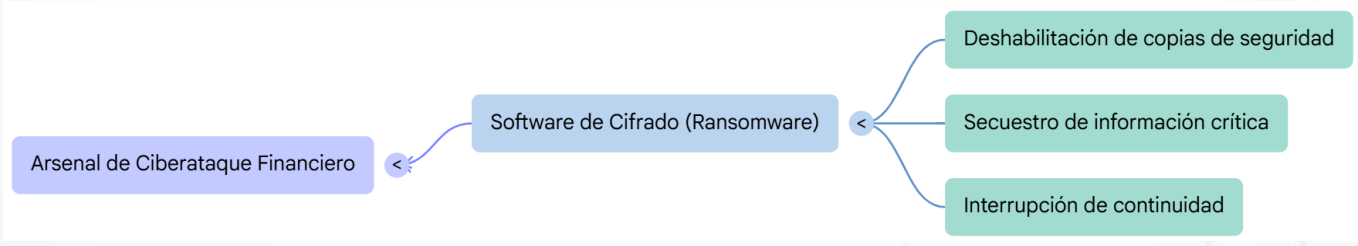
Herramientas y Malware Específico

El arsenal identificado revela una especialización técnica orientada a comprometer la integridad y disponibilidad del ecosistema financiero nacional:

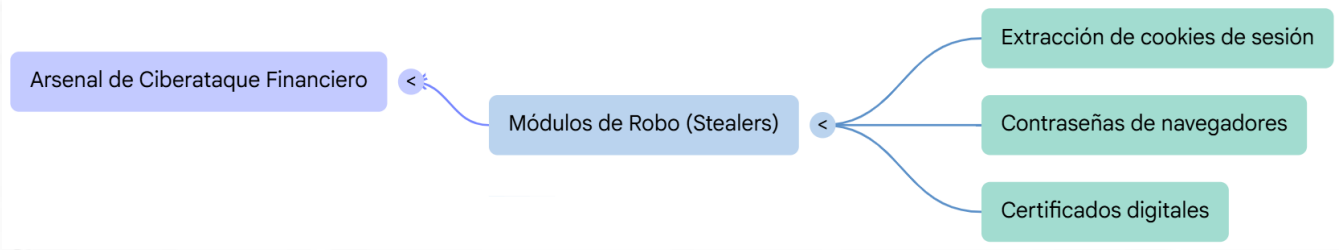
- **Agentes de Control Remoto (RAT):** Software diseñado para otorgar a los atacantes control total sobre las estaciones de trabajo de los empleados, permitiéndoles visualizar pantallas y capturar credenciales de acceso a aplicativos bancarios en tiempo real.



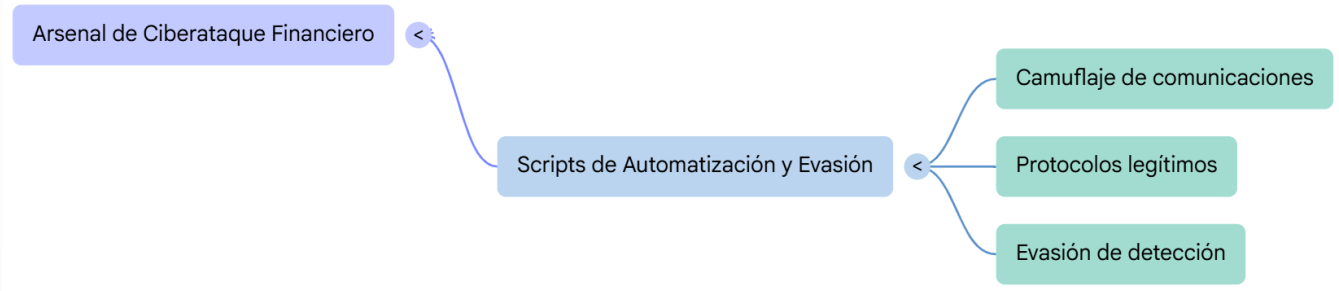
- **Software de Cifrado y Extorsión (Ransomware):** Variantes de última generación configuradas para deshabilitar copias de seguridad y secuestrar información crítica, con el objetivo de interrumpir la continuidad del negocio y presionar a la entidad.



- **Módulos de Robo de Información (Stealers):** Herramientas ligeras enfocadas exclusivamente en la extracción de cookies de sesión, contraseñas almacenadas en navegadores y certificados digitales necesarios para transacciones institucionales.



- **Scripts de Automatización y Evasión:** El uso de códigos personalizados que permiten a las amenazas camuflar sus comunicaciones bajo protocolos legítimos, dificultando su detección por parte de los sistemas de monitoreo tradicionales.

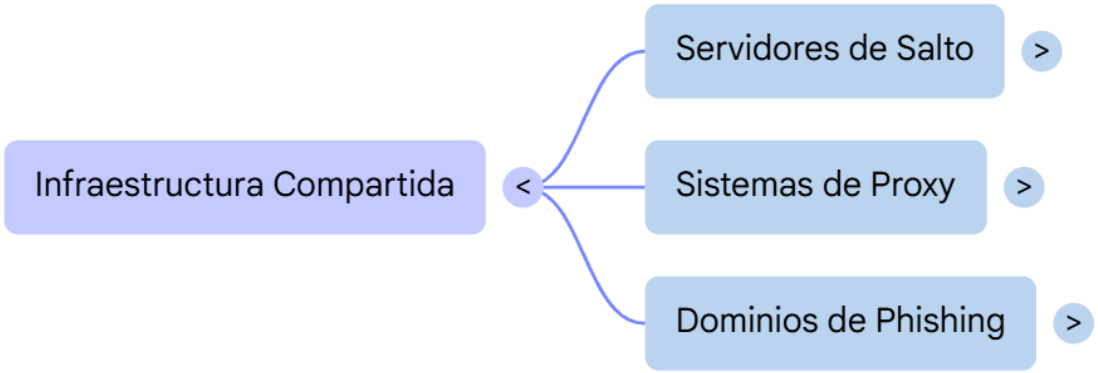


CORRELACIÓN ENTRE ACTORES Y GRUPOS

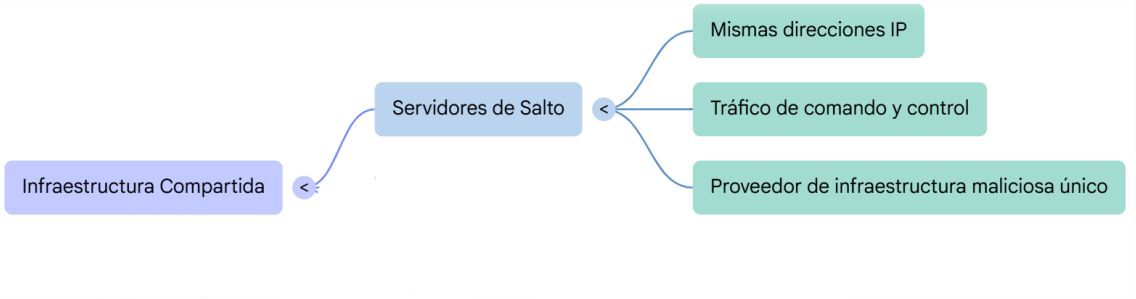
La inteligencia recopilada revela que los adversarios del sector financiero no operan en silos aislados; por el contrario, existe una interconexión táctica donde grupos con objetivos de espionaje (APT) y grupos con fines económicos (Cibercrimen) convergen en el uso de infraestructuras y métodos de intrusión. Esta correlación indica la existencia de un mercado de servicios ilícitos donde el acceso inicial a una red bancaria colombiana puede ser obtenido por un actor y posteriormente vendido a otro para la ejecución de un ransomware o fraude transaccional.

Infraestructura Compartida

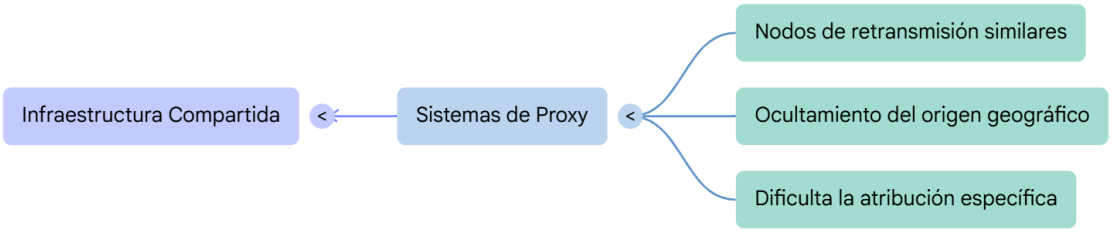
Se ha identificado el uso recurrente de los mismos segmentos de red y proveedores de servicios de alojamiento por parte de múltiples actores. Esta infraestructura compartida se manifiesta a través de:



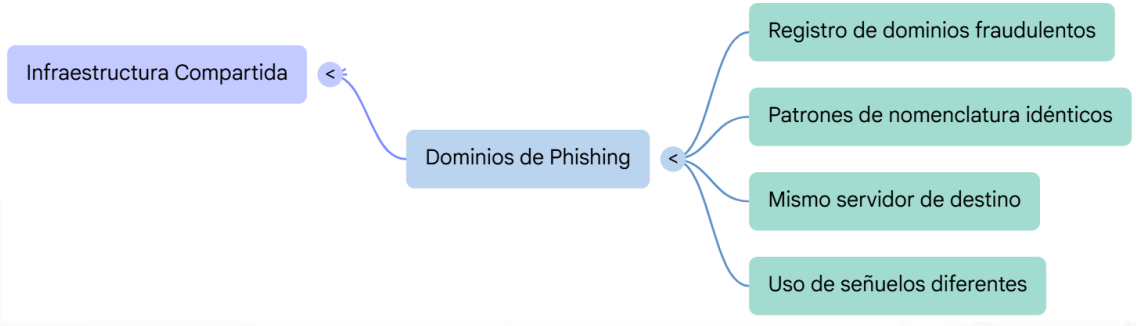
- ✓ **Servidores de Salto:** Uso de las mismas direcciones IP para el tráfico de comando y control, lo que sugiere que varios grupos adquieren servicios de infraestructura maliciosa al mismo proveedor.



- ✓ **Sistemas de Proxy:** Implementación de nodos de retransmisión similares para ocultar el origen geográfico de los ataques, dificultando la atribución específica a un solo grupo.

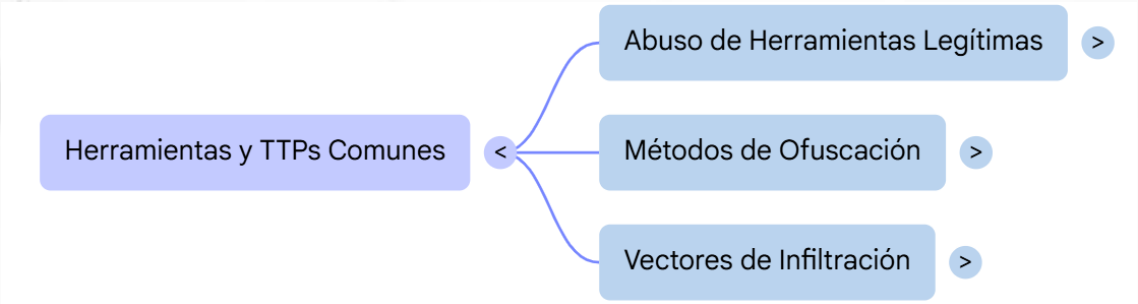


- ✓ **Dominios de Phishing:** Registro de dominios fraudulentos bajo patrones de nomenclatura idénticos, utilizados en campañas que, aunque tienen señuelos diferentes, comparten el mismo servidor de destino.

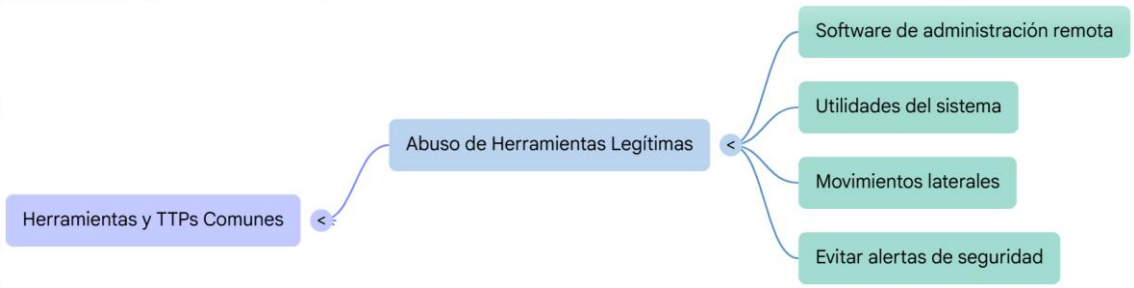


Herramientas y TTPs Comunes

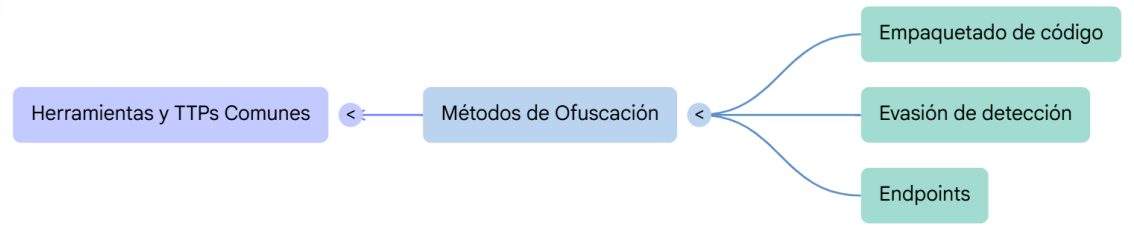
A pesar de tener motivaciones distintas, los grupos detectados emplean Tácticas, Técnicas y Procedimientos (TTPs) estandarizados que facilitan sus operaciones en el entorno financiero:



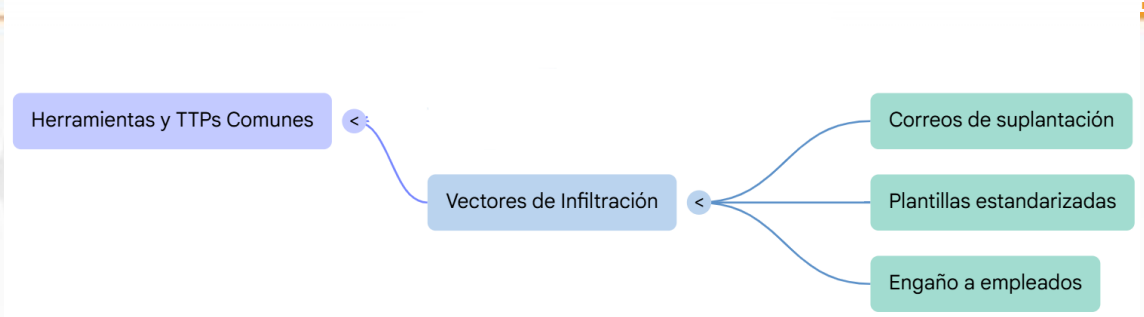
- ✓ **Abuso de Herramientas Legítimas:** El uso de software de administración remota y utilidades del sistema para realizar movimientos laterales sin activar alertas de seguridad.



- ✓ **Métodos de Ofuscación:** Empleo de técnicas de empaquetado de código similares para evadir las soluciones de detección tradicionales en los puntos finales (endpoints).

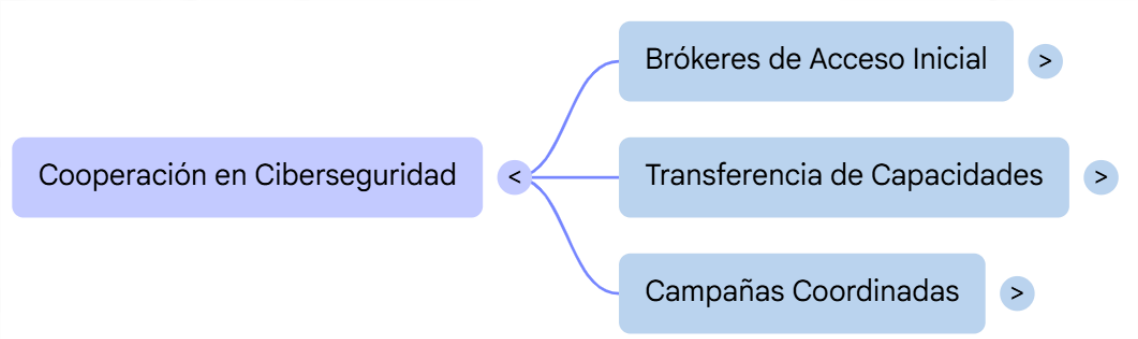


- ✓ **Vectores de Infiltración:** La estandarización de correos electrónicos de suplantación que utilizan plantillas casi idénticas para engañar a los empleados del sector.



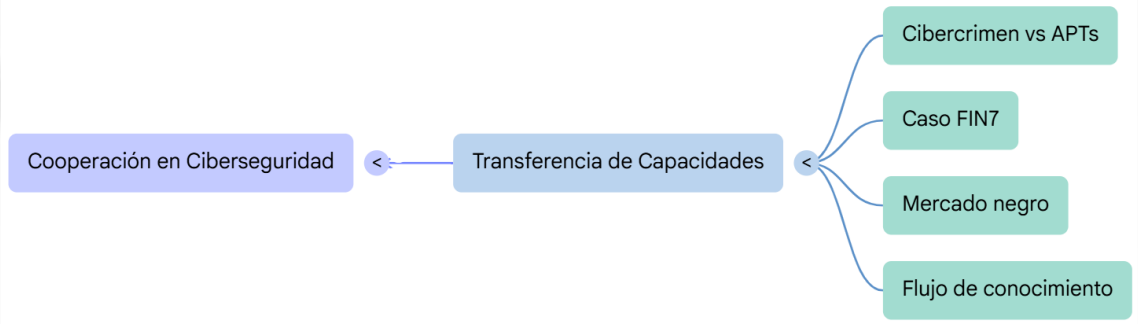
Posibles Colaboraciones o Vínculos

La evidencia técnica sugiere niveles de cooperación que van desde la simple coincidencia de herramientas hasta alianzas operativas:

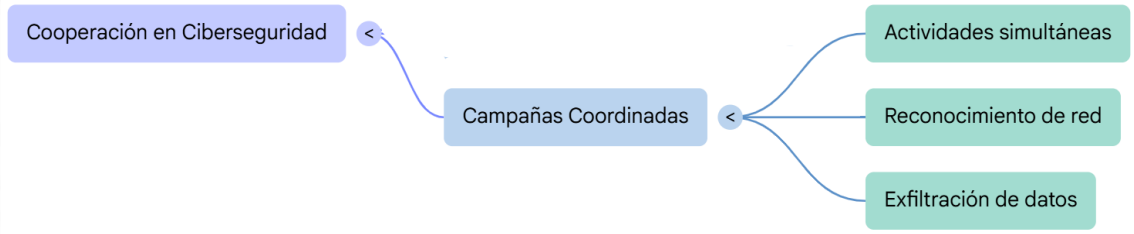


- ✓ **Brókeres de Acceso Inicial**: Actores que se dedican exclusivamente a comprometer redes para luego transferir el control a grupos más especializados en el robo de activos financieros.

- ✓ **Transferencia de Capacidades:** El uso por parte de grupos de cibercrimen (como FIN7) de técnicas previamente reservadas para actores estatales (APTs), lo que demuestra un flujo constante de conocimiento y herramientas en el mercado negro.



- ✓ **Campañas Coordinadas:** Detección de actividades simultáneas donde un grupo realiza el reconocimiento de la red mientras otro prepara el entorno para la exfiltración masiva de datos.



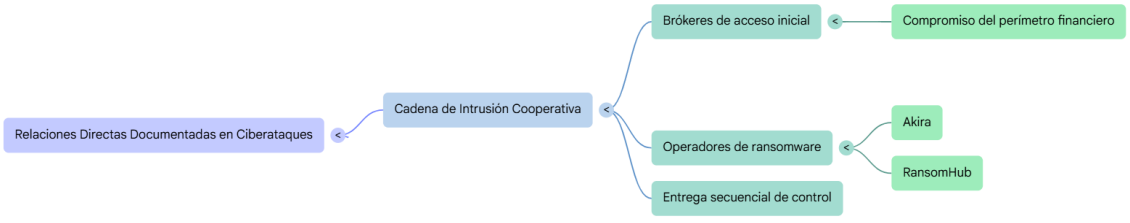
Visualización de relaciones

La visualización de relaciones permite desarticular la complejidad de las operaciones adversarias al mapear las conexiones latentes entre diferentes entidades de amenaza que impactan al sector financiero colombiano. Este análisis de red trasciende la identificación individual de grupos, permitiendo visualizar un ecosistema interdependiente donde la infraestructura y las capacidades técnicas fluyen entre actores, lo que facilita la detección de patrones de ataque sistémicos y la anticipación de movimientos coordinados que buscan comprometer la integridad bancaria.

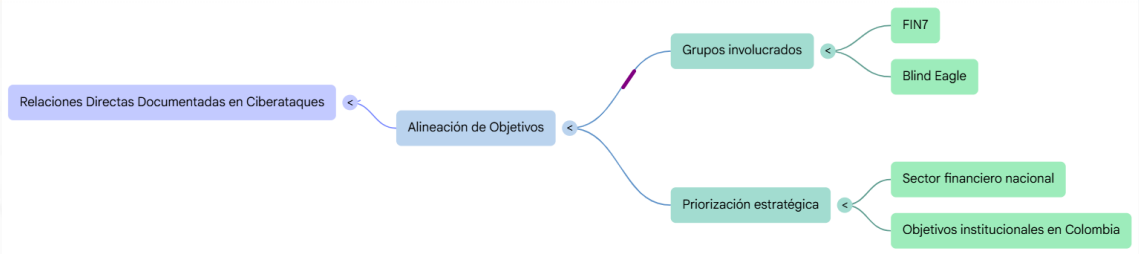
Relaciones directas documentadas:

Existen vínculos operativos explícitos donde la ejecución de una campaña requiere la participación secuencial de varios actores:

- ✓ **Cadena de Intrusión Cooperativa:** Se documenta la relación entre brókeres de acceso inicial y operadores de ransomware (como Akira y RansomHub), donde los primeros comprometen el perímetro financiero para entregar el control a los segundos.

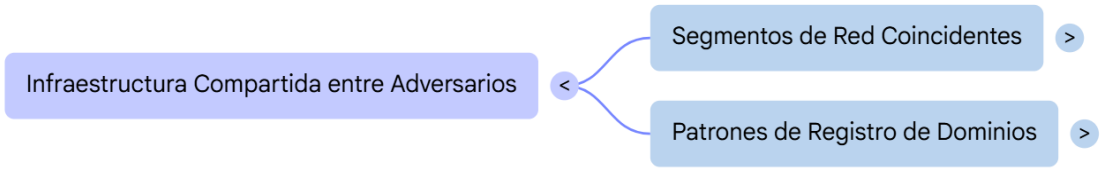


- ✓ **Alineación de Objetivos:** Grupos como FIN7 y Blind Eagle presentan coincidencias directas en la selección de objetivos institucionales en Colombia, lo que sugiere una priorización estratégica compartida del sector financiero nacional.

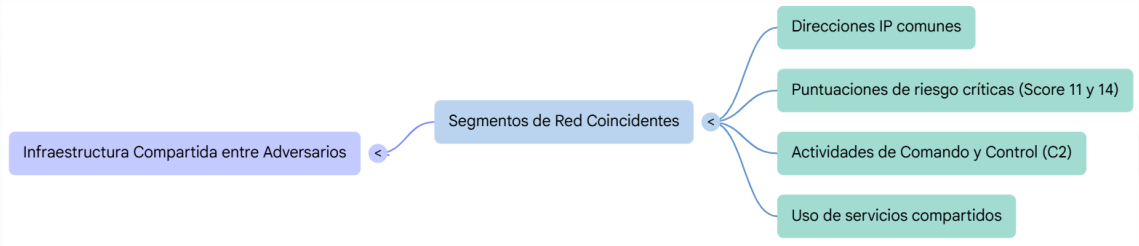


Relaciones por la infraestructura compartida

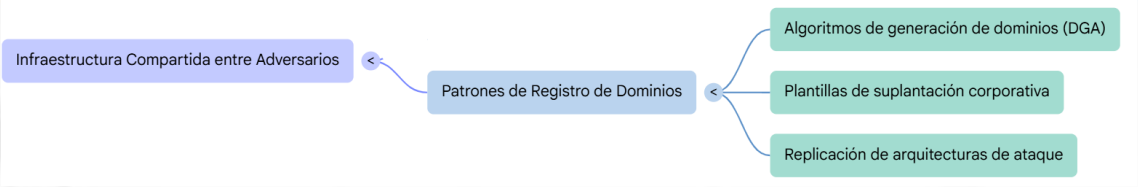
La infraestructura técnica actúa como el nexo común más frecuente entre los adversarios detectados:



- ✓ **Segmentos de Red Coincidentes:** Varios actores utilizan las mismas direcciones IP con puntuaciones de riesgo críticas (Score 11 y 14) para actividades de comando y control (C2), indicando el uso de servicios compartidos de infraestructura maliciosa.

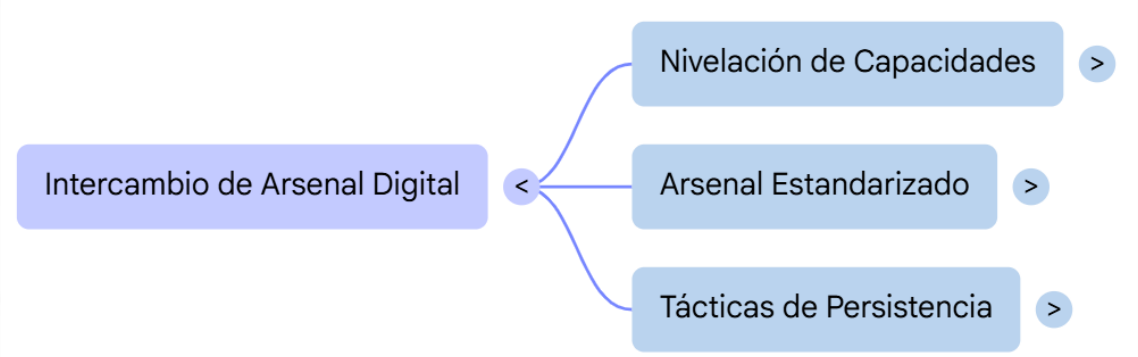


- ✓ **Patrones de Registro de Dominios:** La similitud en los algoritmos de generación de dominios (DGA) y en las plantillas de suplantación de servicios corporativos sugiere que distintos grupos adquieren o replican las mismas arquitecturas de ataque.

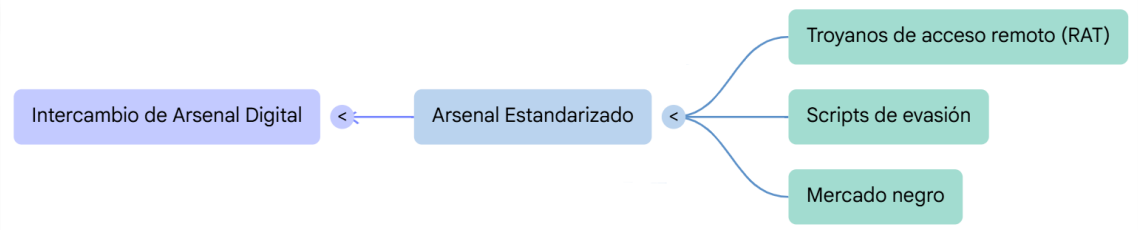


Relaciones por herramientas comunes

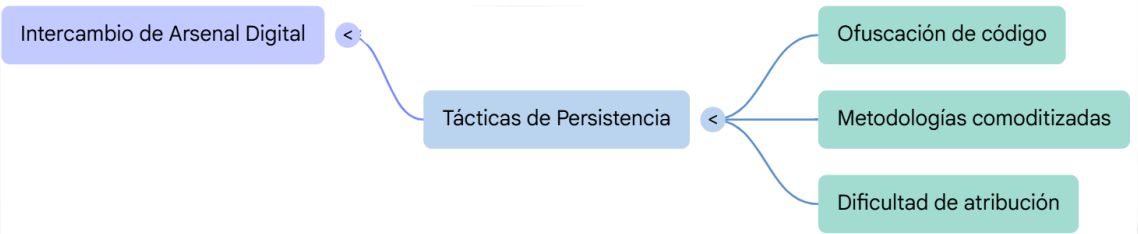
El intercambio de arsenal digital nivela las capacidades de grupos con distintas motivaciones:



- ✓ **Arsenal Estandarizado:** El uso transversal de troyanos de acceso remoto (RAT) y scripts de evasión por parte de actores tanto estatales (APTs) como financieros evidencia un flujo constante de herramientas en el mercado negro.

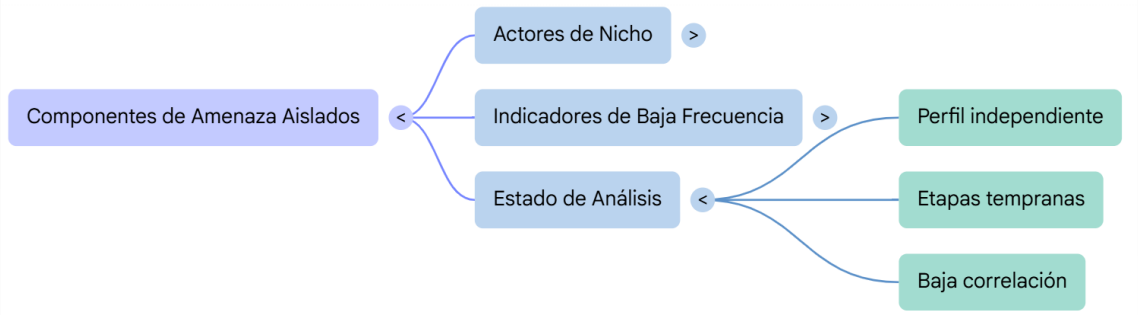


- ✓ **Tácticas de Persistencia:** La adopción de técnicas de ofuscación de código idénticas entre diversos grupos dificulta la atribución y confirma la existencia de metodologías de ataque "comoditizadas" para el sector financiero.

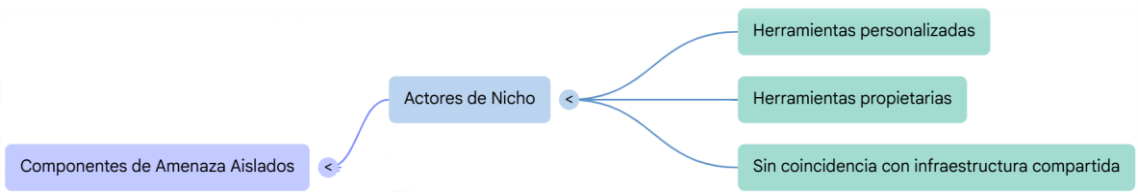


Nodos aislados o con baja correlación (por ahora):

Algunos componentes de la amenaza mantienen un perfil de operación independiente o se encuentran en etapas tempranas de análisis:



- ✓ **Actores de Nicho:** Grupos con herramientas personalizadas y propietarias que no muestran coincidencias con la infraestructura compartida detectada en el grueso de los indicadores.

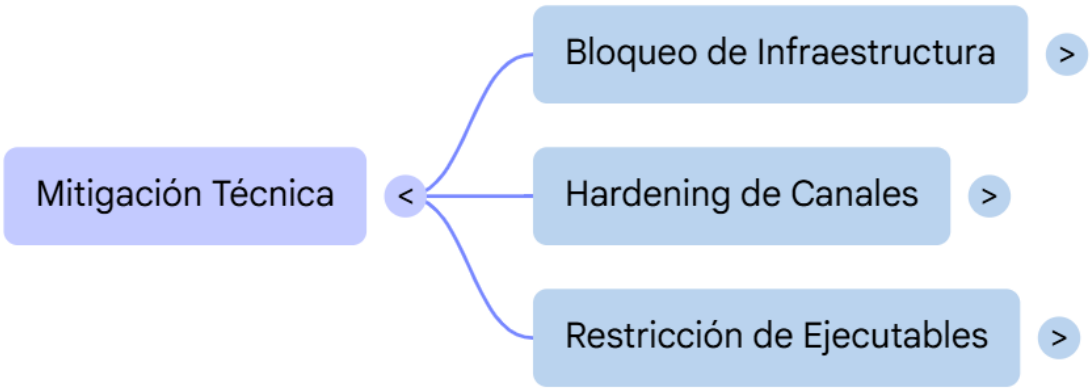


- ✓ **Indicadores de Baja Frecuencia:** Ciertos activos de red y URLs de descarga que, debido a su reciente aparición o alta especificidad, no han permitido establecer vínculos robustos con las redes de ataque ya documentadas.

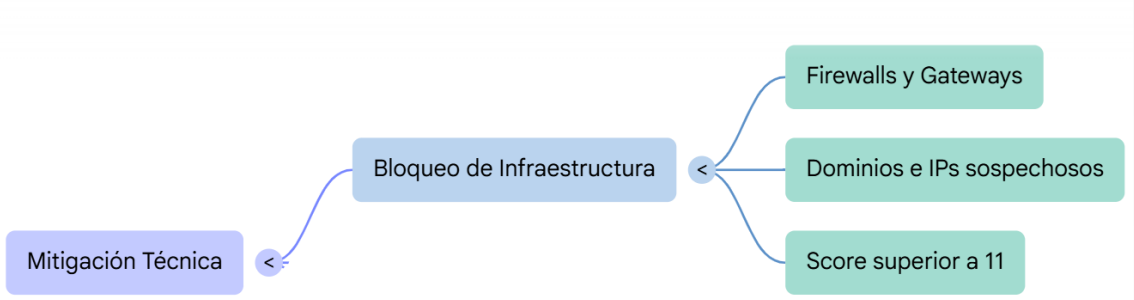
RECOMENDACIONES ESTRATÉGICAS

El panorama actual exige una transición de una postura de seguridad reactiva a una de Defensa Proactiva. A continuación, se detallan las líneas de acción prioritarias:

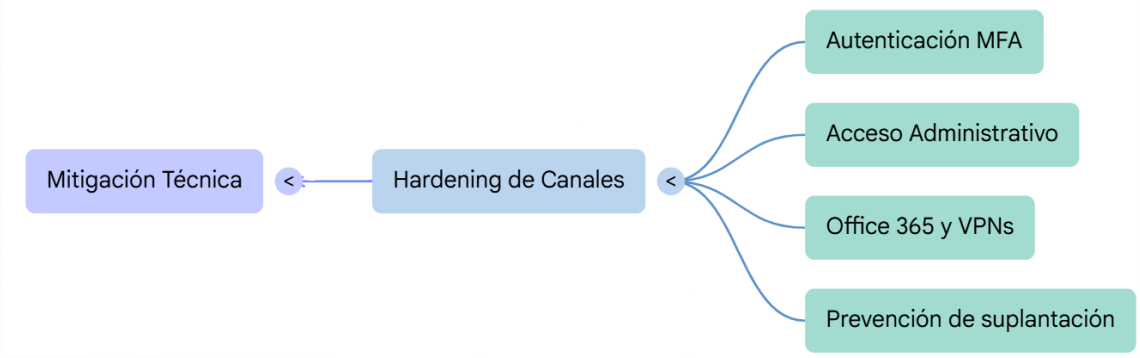
Recomendaciones de Mitigación Técnica



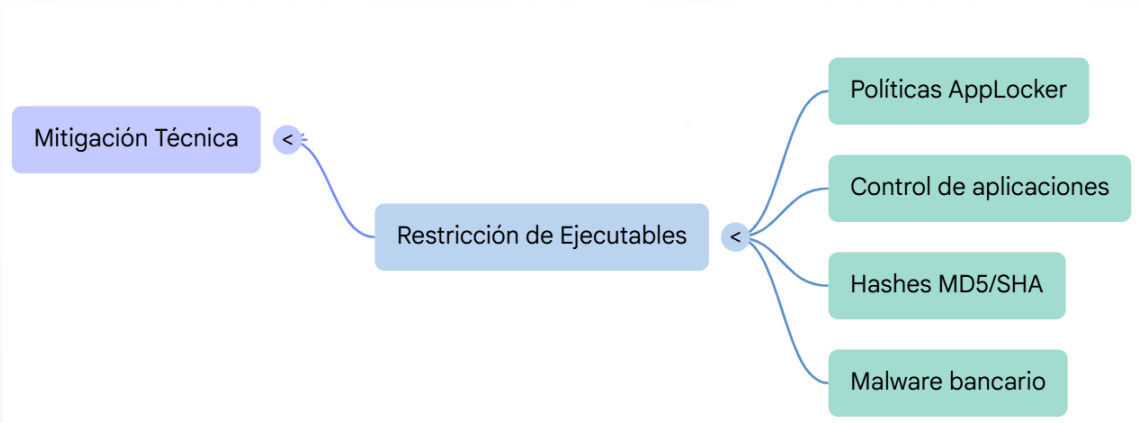
- ✓ **Bloqueo de Infraestructura Crítica:** Implementar reglas de bloqueo inmediato en Firewalls y Web Gateways para los dominios y direcciones IP con Score superior a 11 identificados en este informe.



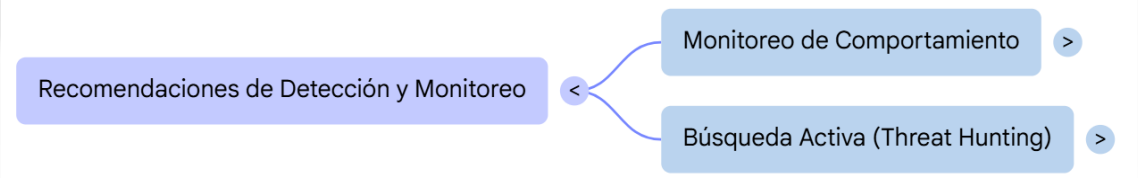
- ✓ **Hardening de Canales Digitales: Reforzar** la autenticación multifactor (MFA) no solo para clientes, sino especialmente para el acceso administrativo y de empleados a servicios de Office 365 y VPNs, dado el alto volumen de suplantación de estas plataformas.



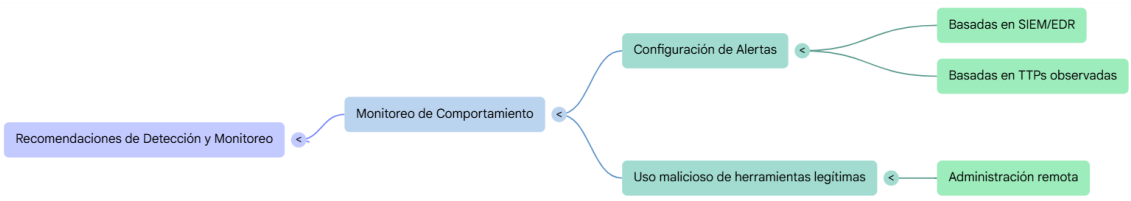
- ✓ **Restricción de Ejecutables:** Implementar políticas de control de aplicaciones (AppLocker o similares) para evitar la ejecución de archivos sospechosos asociados a los hashes (MD5/SHA) reportados como malware bancario.



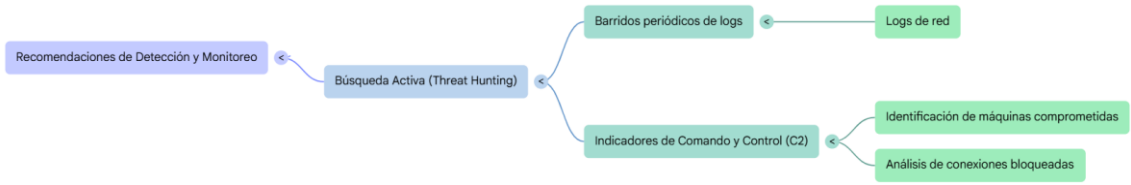
Recomendaciones de Detección y Monitoreo



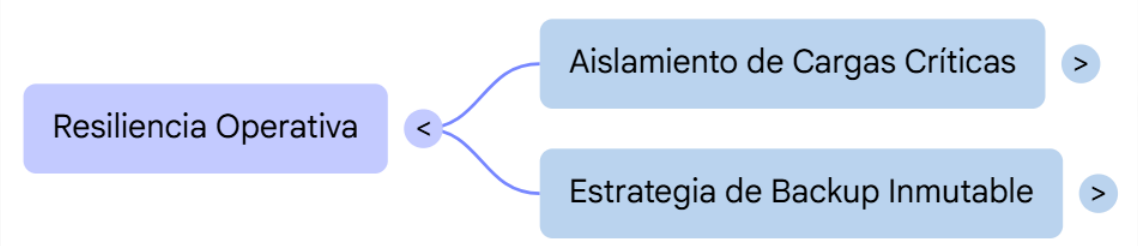
- ✓ **Monitoreo de Comportamiento:** Configurar alertas de SIEM/EDR basadas en las TTPs observadas, como el uso de herramientas de administración remota legítimas para fines maliciosos.



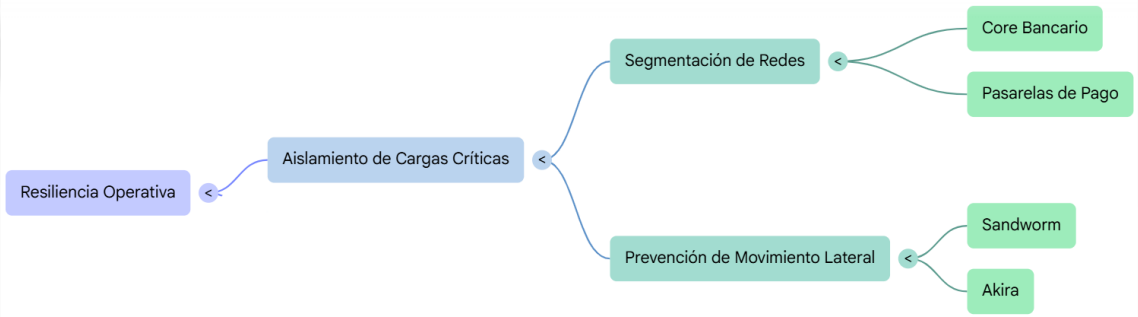
- ✓ **Búsqueda Activa (Threat Hunting):** Realizar barridos periódicos en los logs de red buscando conexiones hacia los indicadores de Comando y Control (C2) documentados, incluso si la conexión fue bloqueada, para identificar posibles máquinas ya comprometidas.



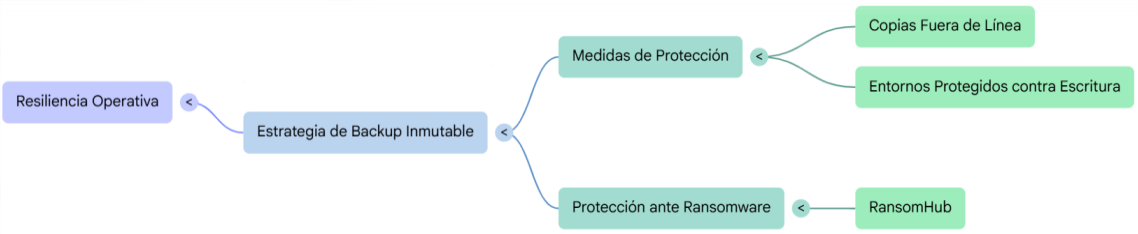
Recomendaciones de Resiliencia Operativa



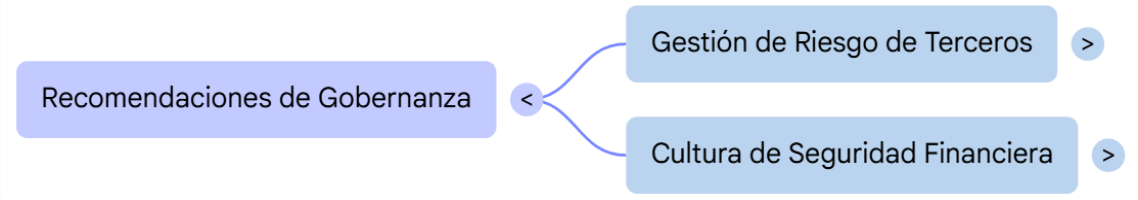
- ✓ **Aislamiento de Cargas Críticas:** Segmentar las redes que gestionan el core bancario y las pasarelas de pago para evitar el movimiento lateral de actores como Sandworm o Akira.



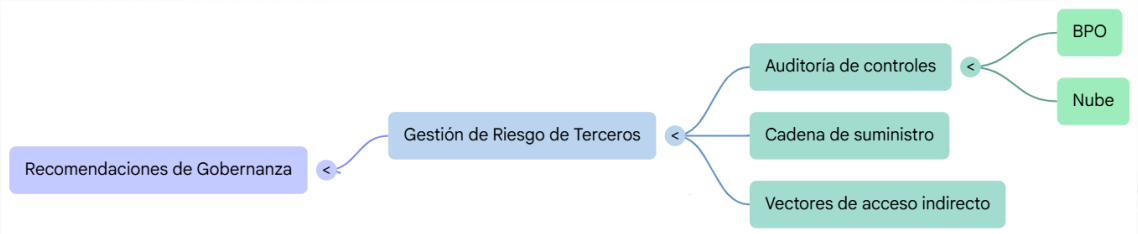
- ✓ **Estrategia de Backup Inmutable:** Asegurar que las copias de seguridad estén fuera de línea o en entornos protegidos contra escritura, como medida de protección ante el ransomware RansomHub.



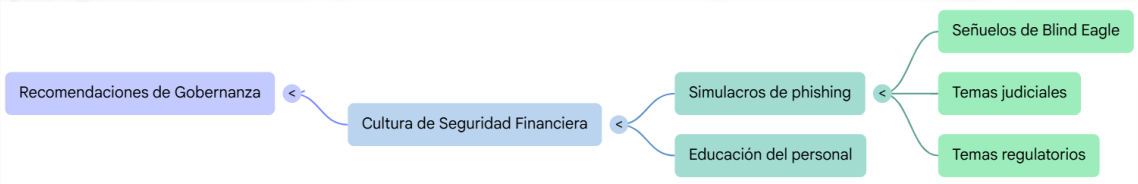
Recomendaciones de Gobernanza



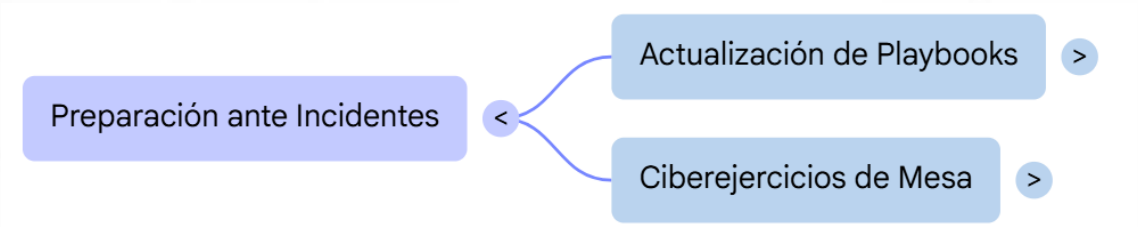
- ✓ **Gestión de Riesgo de Terceros:** Auditar los controles de ciberseguridad de proveedores críticos (BPO y Nube), ya que la cadena de suministro es un vector de acceso indirecto identificado.



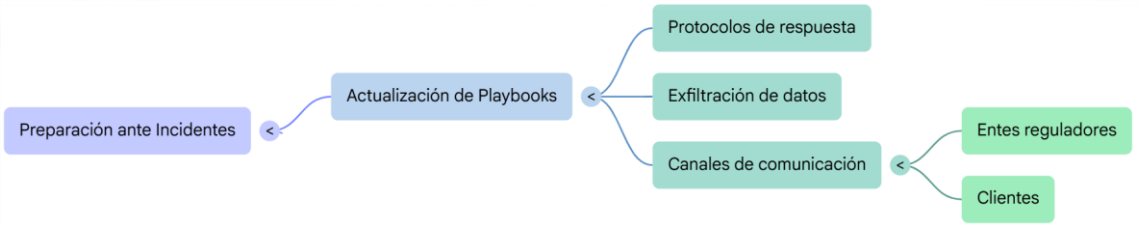
- ✓ **Cultura de Seguridad Financiera:** Ejecutar simulacros de phishing que repliquen los señuelos específicos utilizados por Blind Eagle (temas judiciales y regulatorios colombianos) para educar al personal.



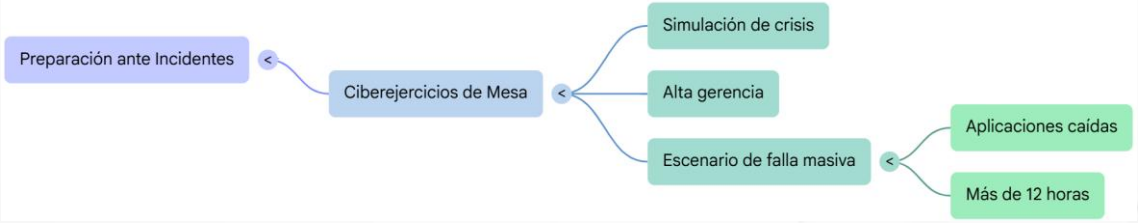
Preparación ante Incidentes



- ✓ **Actualización de Playbooks:** Revisar los protocolos de respuesta específicamente para incidentes de exfiltración de datos, definiendo canales de comunicación claros con los entes reguladores y clientes.

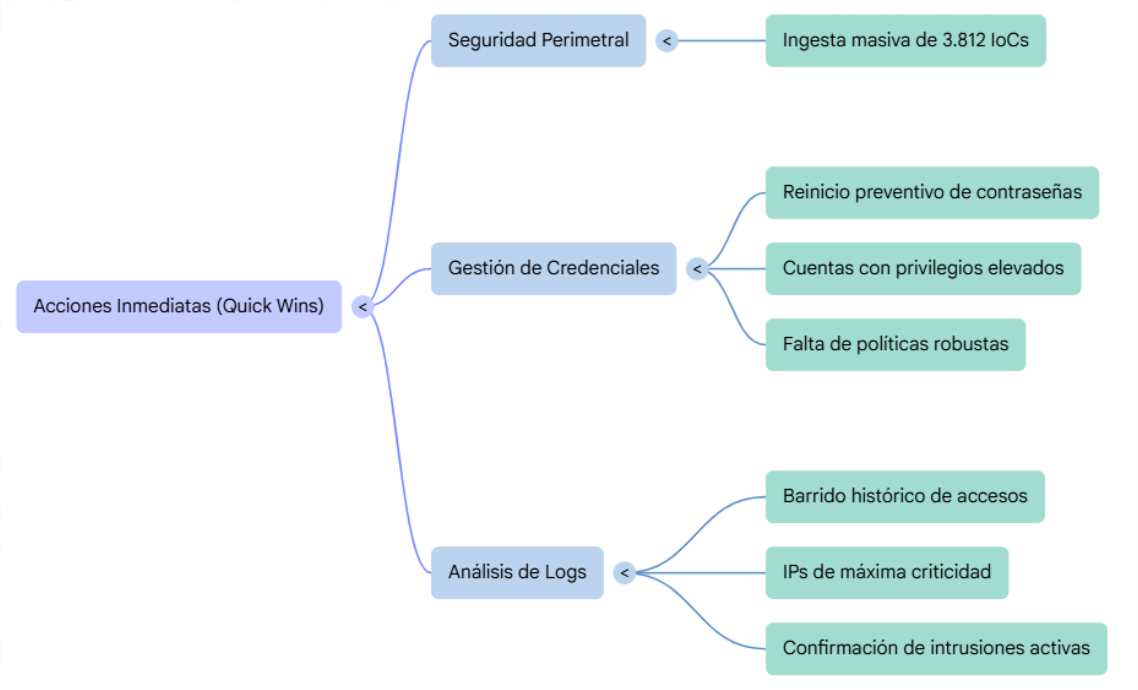


- ✓ **Ciber ejercicios de Mesa (Tabletop):** Realizar ejercicios de simulación de crisis con la alta gerencia basados en un escenario de falla masiva de aplicaciones por más de 12 horas, similar a los eventos reportados recientemente.



Acciones Inmediatas (Quick Wins)

Como medidas de ejecución urgente, se debe proceder con la ingesta masiva de los 3.812 indicadores de compromiso (IoCs) en todas las soluciones de seguridad perimetral de la entidad. De igual manera, se requiere un reinicio preventivo de credenciales para todas las cuentas con privilegios elevados que no cuenten con políticas de acceso robustas.



Finalmente, es prioritario realizar un barrido histórico en los logs de acceso en busca de interacciones con las direcciones IP de máxima criticidad detectadas en el análisis para confirmar que no existan intrusiones activas en este momento.

CONCLUSIONES

1. **Implementación de Bloqueo Proactivo de Infraestructura**
   - Es fundamental realizar la ingesta automatizada de los IoCs de alta criticidad (aquellos con Score 11 y 14) en las soluciones perimetrales como Firewalls,

     Proxies y Web Gateways. Dado que se han detectado más de 3.200 activos de red maliciosos (Dominios e IPs), el bloqueo preventivo de estos puntos de Comando y Control (C2) es la primera línea de defensa para evitar que un sistema comprometido se comunique con el atacante.

2. Endurecimiento de la Autenticación de Identidades

- Ante el volumen masivo de campañas de phishing dirigidas a recolectar credenciales (usando dominios como microsoft-um.xyz u office365-management.com), se debe exigir el uso de Autenticación Multifactor (MFA) en todos los niveles. Esto incluye no solo el acceso de clientes a la banca en línea, sino de manera crítica el acceso administrativo de empleados a correos corporativos y redes privadas virtuales (VPN).

3. Blindaje contra Malware Bancario y Ransomware

- Se recomienda implementar políticas de Control de Aplicaciones (Allowlisting) para evitar la ejecución de archivos sospechosos asociados a las firmas (Hashes) detectadas de agentes como Akira, RansomHub y AsyncRAT. Estas herramientas están diseñadas específicamente para el robo de activos y el secuestro de información operativa en el entorno financiero nacional.

4. Monitoreo de Tácticas de Evasión y Movimiento Lateral

- Los adversarios están utilizando herramientas legítimas de administración remota para camuflarse. Las entidades deben configurar sus sistemas de detección (EDR/SIEM) para generar alertas sobre comportamientos anómalos, como el uso de herramientas de sistema para reconocimiento de red o intentos de conexión desde IPs con reputación maliciosa documentadas en el informe.

5. Mitigación del Riesgo de Suplantación Judicial y Regulatoria

- Debido a que el grupo Blind Eagle (APT-C-36) utiliza señuelos específicos de la Fiscalía o la DIAN para infiltrar redes colombianas, es vital realizar campañas de concientización focalizadas. Los empleados deben ser entrenados para identificar estos vectores de ataque locales, que representan uno de los mayores riesgos de acceso inicial para el sector.

6. Estrategia de Resiliencia y Respaldo Inmutable

- Para contrarrestar el impacto de grupos de doble extorsión como RansomHub, las instituciones deben asegurar que sus copias de seguridad sean inmutables o estén fuera de línea. Esto garantiza que, ante un cifrado masivo de servidores, la entidad pueda restaurar sus servicios críticos sin ceder ante las demandas económicas de los atacantes.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **APT (Advanced Persistent Threat):** Grupos de ataque organizados (como Blind Eagle o Sandworm) que mantienen una presencia prolongada y sofisticada en redes críticas para espionaje o sabotaje.
- **Adversario (Adversary):** Grupo o individuo con alta capacidad técnica que realiza acciones maliciosas (fraude, robo de datos) contra las entidades financieras.
- **IoC (Indicador de Compromiso):** Evidencia técnica digital (IP, dominio o hash) que permite identificar y rastrear actividades maliciosas en la infraestructura.
- **Score de Criticidad:** Valor numérico (escala 1-15) que determina la peligrosidad de un indicador; puntuaciones de 11 a 14 se consideran niveles críticos en este informe.
- **TTPs (Tácticas, Técnicas y Procedimientos):** Descripción del comportamiento y metodologías operativas que describen cómo un adversario ejecuta un ataque de principio a fin.
- **MITRE ATT&CK:** Marco global de referencia que clasifica y describe las tácticas y técnicas de los atacantes basándose en observaciones del mundo real.
- **Bróker de Acceso Inicial:** Actores (como Raspberry Robin) que comprometen redes para luego vender ese acceso a operadores de ransomware o grupos de fraude financiero.

Infraestructura y Redes

- **C2 (Command and Control):** Servidores externos utilizados por los atacantes para enviar instrucciones y recibir datos de los sistemas infectados dentro del banco.
- **FQDN (Fully Qualified Domain Name):** Nombre completo de un dominio en internet (ej. microsoft-um.xyz) que identifica un activo de red utilizado en campañas de phishing o control.
- **DGA (Domain Generation Algorithm):** Técnica donde el malware genera múltiples nombres de dominio aleatorios para ocultar sus comunicaciones y evadir bloqueos.
- **Superficie de Ataque:** Todos los puntos de exposición (canales digitales, pagos inmediatos, nube) donde una entidad financiera puede ser vulnerada.
- **Core Bancario:** Sistemas centrales que procesan las transacciones financieras principales; son considerados cargas críticas de alta prioridad para la protección.
- **Pasarelas de Pago:** Plataformas tecnológicas que autorizan pagos y transacciones, identificadas como objetivos principales para comprometer la integridad financiera.

Herramientas y Malware

- **Ransomware:** Software malicioso (ej. Akira, RansomHub) que cifra la información y exige un rescate, a menudo utilizando modelos de "doble extorsión" (cifrado y filtración).
- **RAT (Remote Access Trojan):** Troyanos de acceso remoto utilizados para capturar credenciales y tomar control de estaciones de trabajo de empleados en tiempo real.
- **Stealer:** Módulos de malware enfocados exclusivamente en el robo de cookies de sesión, contraseñas de navegadores y certificados digitales.
- **Malware Bancario:** Código especializado en infiltrar infraestructuras financieras para facilitar el fraude transaccional y el robo de activos.
- **Hash (MD5, SHA-1, SHA-256):** Huella digital única de un archivo que permite identificar piezas de malware específicas sin importar su nombre.
- **Phishing:** Técnica de ingeniería social que suplanta servicios legítimos (Microsoft, DIAN, Fiscalía) para robar credenciales de acceso.

Sector Financiero y Resiliencia

- **Estabilidad y Confianza Sistémica:** Capacidad del sector financiero para operar sin interrupciones, protegiendo los activos y la información de los ahorradores colombianos.
- **Finanzas Abiertas (Open Banking):** Modelo de intercambio de datos financieros que incrementa la interdependencia entre instituciones y expande la superficie de exposición.
- **Resiliencia Cibernética:** Capacidad de una entidad para resistir, absorber y recuperarse de ataques dirigidos, manteniendo la continuidad de sus servicios.
- **Backup Inmutable:** Copias de seguridad protegidas contra escritura o fuera de línea, diseñadas para garantizar la recuperación ante ataques de ransomware.
- **Hardening:** Proceso de asegurar un sistema mediante la reducción de su superficie de vulnerabilidad y el refuerzo de sus controles (como MFA en VPNs).

El **ColCERT** tiene la misión de liderar y coordinar la gestión de incidentes, la identificación de vulnerabilidades, riesgos y amenazas contra la seguridad digital nacional. Actuamos como punto central de contacto y colaboración entre entidades públicas, privadas y la comunidad internacional, fortaleciendo la resiliencia del Estado mediante el intercambio de información, el desarrollo de capacidades, la difusión de lineamientos, la identificación de infraestructuras críticas y la promoción de una cultura de seguridad, a través de la cooperación nacional e internacional.

Más allá de la gestión ante amenazas, el **ColCERT** fortalece la seguridad digital del país mediante acciones de prevención, orientación y generación de capacidades dirigidas a entidades públicas, privadas y ciudadanía, contribuyendo a una transformación digital más segura y resiliente en Colombia.

Conéctate con el ColCERT

Reporte de incidentes:
csirtgob@mintic.gov.co
Entidades de Gobierno

contacto@colcert.gov.co
Privados

icc@colcert.gov.co
Temas de ICC

Sitio web
https://www.colcert.gov.co
Alertas y boletines

@colCERT

Línea directa:
+57 601 344 2222