
TIC
Informe
de apreciación
Sector TIC
COLCERT

Contenido

Informe de apreciación
Sector TIC colombiano

Abril del 2026

IN-20260523-030

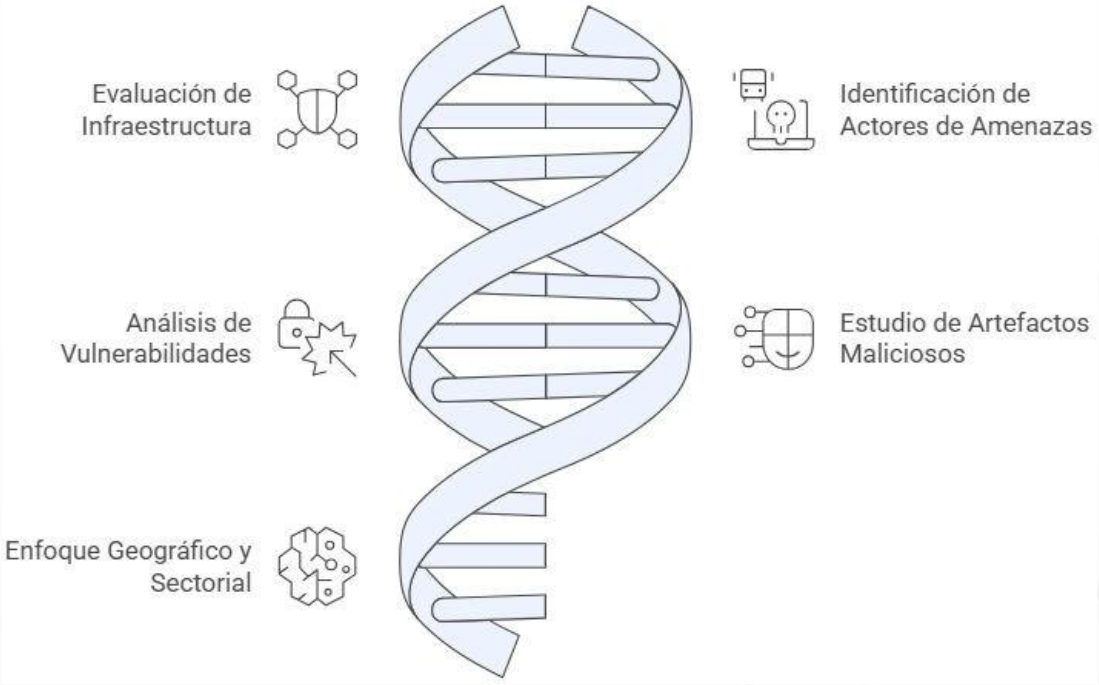
TLP: CLEAR

INTRODUCCIÓN

El entorno digital de Colombia se encuentra en una etapa de transformación acelerada, lo que ha posicionado al sector de Tecnologías de la Información y las Comunicaciones (TIC) como un pilar fundamental para el desarrollo económico, pero también como un objetivo de alto valor para actores de amenazas sofisticados. Este informe surge de la necesidad de analizar y comprender las dinámicas de ataque que impactan específicamente a la infraestructura tecnológica y de telecomunicaciones del país. A través de la correlación de datos técnicos y telemetría de amenazas, se busca ofrecer una perspectiva clara sobre los métodos de operación de diversos grupos adversarios, permitiendo a las organizaciones del sector anticiparse a posibles incidentes y fortalecer su resiliencia operativa ante un ecosistema de riesgos en constante evolución.

Componentes del Análisis:

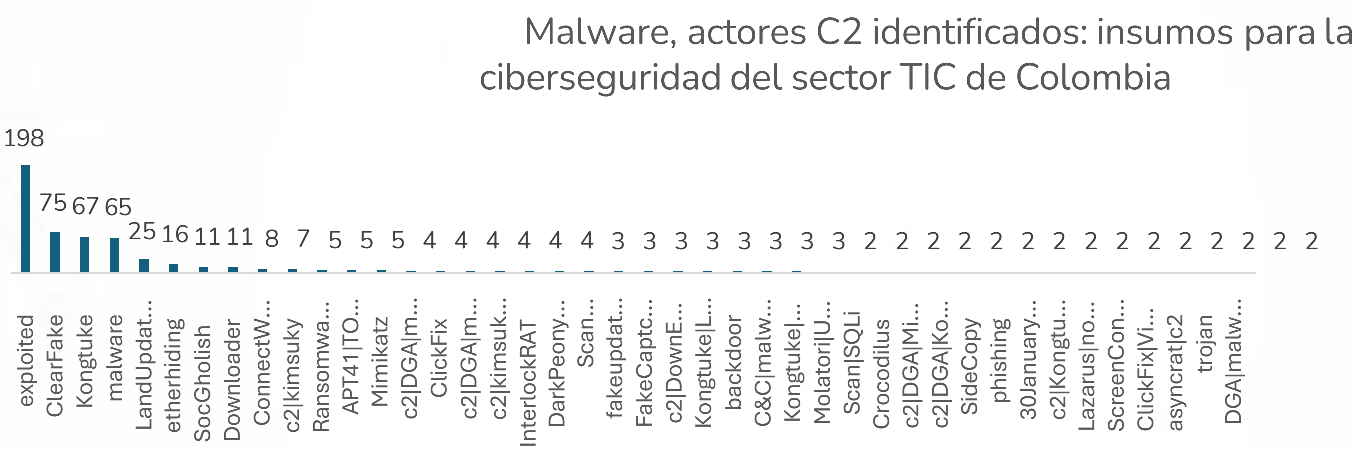
- **Evaluación de Infraestructura de Comando y Control:** Análisis exhaustivo de nombres de dominio y direcciones IP utilizados para la gestión de ataques y la exfiltración de información sensible.
- **Identificación de Actores de Amenazas:** Caracterización de grupos adversarios con capacidades avanzadas que han demostrado un interés persistente en los activos digitales colombianos.
- **Análisis de Vulnerabilidades Explotadas:** Revisión de fallos de seguridad críticos que están siendo utilizados como puerta de enlace para comprometer redes y servicios tecnológicos.
- **Estudio de Artefactos Maliciosos:** Catalogación de firmas de archivos y software no autorizado diseñado para evadir medidas de detección tradicionales en el sector TIC.
- **Enfoque Geográfico y Sectorial:** Delimitación del estudio a la actividad detectada dentro del territorio nacional, asegurando que los hallazgos sean accionables para el contexto local.

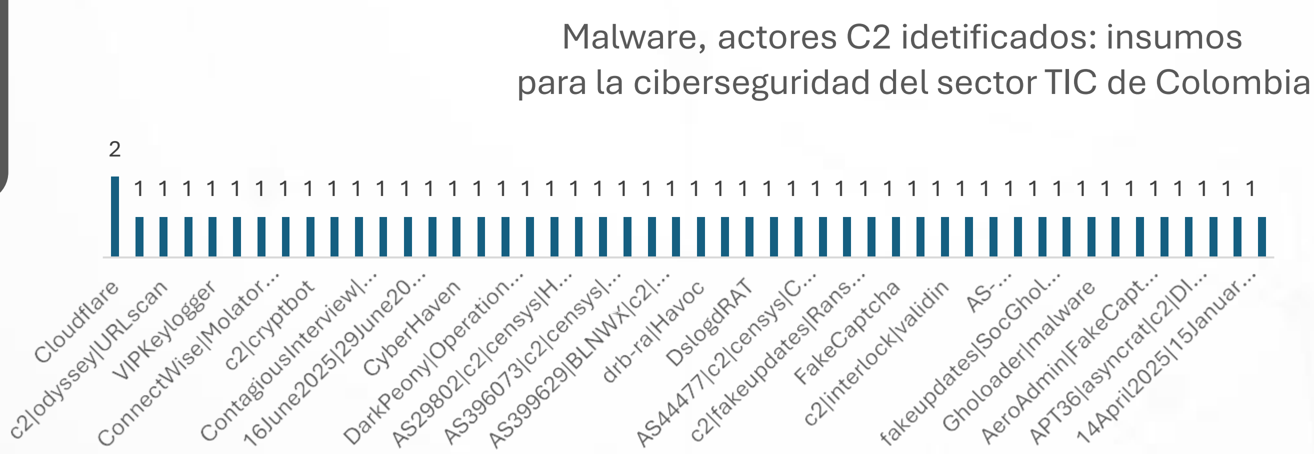


RESUMEN EJECUTIVO

El presente resumen ejecutivo ofrece un análisis detallado sobre el panorama de amenazas identificado para el sector de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, fundamentado en la actividad técnica y operativa registrada recientemente. A través del estudio de miles de indicadores de compromiso, se examina la convergencia de infraestructura maliciosa y tácticas de adversarios especializados que buscan explotar la superficie de ataque de las redes nacionales. Este documento sintetiza los hallazgos críticos relacionados con la exposición de activos digitales y la persistencia de actores de amenazas, con el propósito de orientar la toma de decisiones estratégicas y fortalecer la postura de seguridad frente a campañas dirigidas a la infraestructura crítica tecnológica del país.

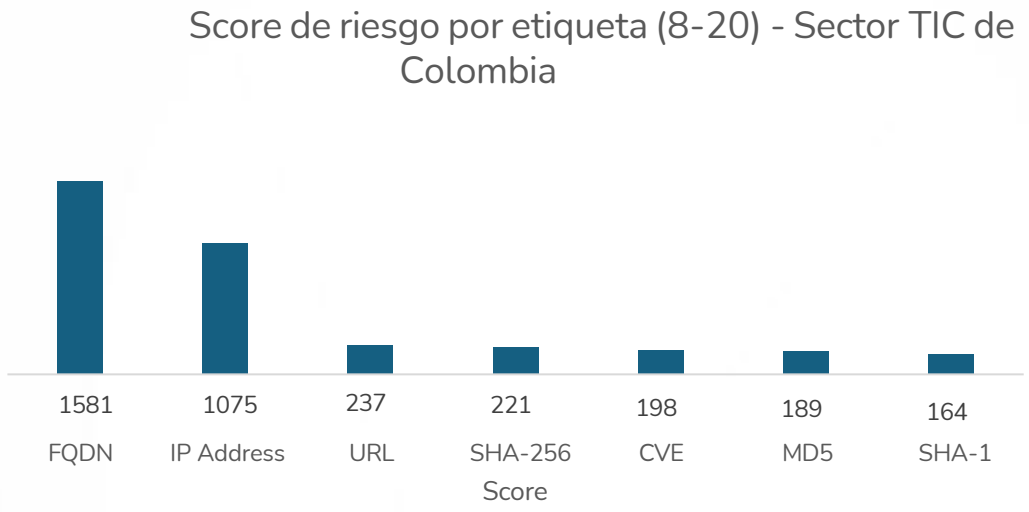
Hallazgos Clave





- **Concentración de Amenazas en Infraestructura de Red:** Se identifica un volumen significativo de indicadores asociados a nombres de dominio (FQDN) y direcciones IP, lo que sugiere una infraestructura de ataque activa dirigida a los servicios de conectividad y plataformas digitales del sector.

- **Persistencia de Actores Especializados:** Se observa la actividad recurrente de grupos con altas capacidades técnicas que dirigen sus operaciones hacia sectores estratégicos, con un enfoque particular en la exfiltración de datos y el espionaje industrial.
- **Explotación de Vulnerabilidades Conocidas:** El registro de múltiples entradas relacionadas con vulnerabilidades (CVE) indica que los atacantes continúan aprovechando fallos de seguridad no mitigados en sistemas operativos y aplicaciones de uso común en el sector tecnológico.
- **Diversidad de Vectores de Compromiso:** La presencia de diversos tipos de archivos maliciosos (hashes) confirma el uso de campañas de malware polimórfico diseñadas para evadir controles de seguridad perimetral tradicionales.



Recomendaciones Prioritarias

- **Fortalecimiento del Monitoreo de Red:** Implementar una vigilancia estricta sobre las resoluciones de dominio y el tráfico saliente hacia direcciones IP con reputación comprometida para detectar comunicaciones de comando y control en etapas tempranas.
- **Gestión Crítica de Parches:** Priorizar la remediación de vulnerabilidades expuestas en activos orientados a internet, especialmente aquellas que permiten la ejecución remota de código o la escalación de privilegios.
- **Validación de Integridad de Archivos:** Reforzar las políticas de inspección de archivos en puntos finales (endpoints) para identificar y bloquear la ejecución de componentes maliciosos detectados en el sector.

Conclusión Estratégica

El sector TIC en Colombia enfrenta un panorama de amenazas caracterizado por la precisión y la persistencia. La alta frecuencia de indicadores relacionados con infraestructura de red demuestra que los adversarios buscan comprometer la base de la cadena de suministro digital. Es imperativo transitar hacia un modelo de defensa proactiva que integre la inteligencia de amenazas en la toma de decisiones operativa para salvaguardar la soberanía tecnológica y la continuidad del servicio.

OBJETIVO Y ALCANCE

Objetivo

Proporcionar una visión estratégica y técnica sobre el panorama de amenazas cibernéticas que afectan al sector TIC en Colombia, analizando los patrones de ataque y los vectores de compromiso más relevantes para facilitar la implementación de medidas preventivas y de mitigación efectivas.

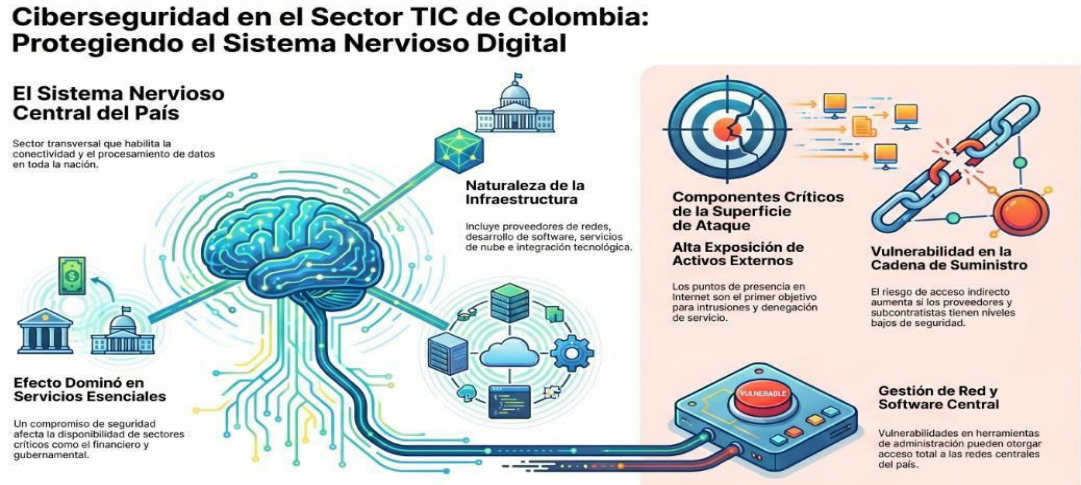
Alcance

Este informe abarca el análisis de **3,665 indicadores de compromiso recolectados recientemente,** los cuales están vinculados específicamente a incidentes, campañas y actores de amenazas con intereses documentados en Colombia y, de manera específica, en las industrias de tecnología y telecomunicaciones. El análisis incluye la revisión de infraestructura maliciosa, firmas de archivos y vulnerabilidades críticas explotadas.

Este informe abarca:

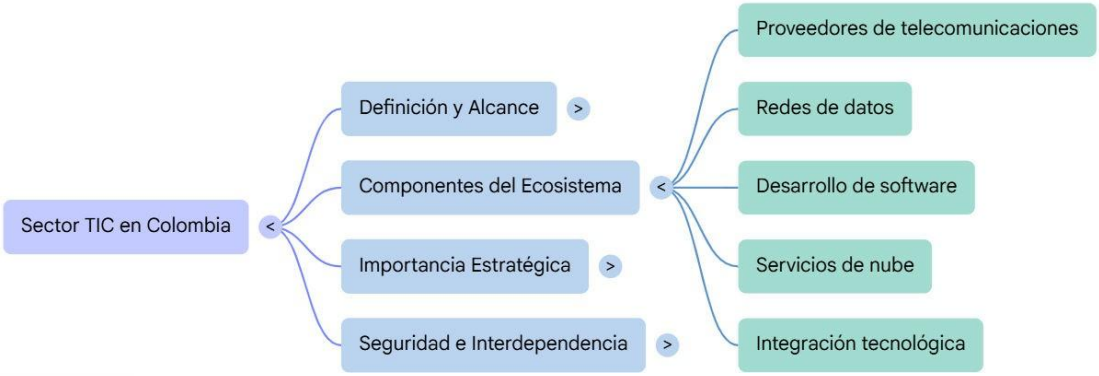
- Identificación de Infraestructura Maliciosa: Comprende el análisis de más de 1,500 nombres de dominio (FQDN) y 1,000 direcciones IP activas vinculadas a operaciones de comando y control.
- Evaluación de Vectores de Intrusión: Incluye la revisión de cerca de 200 registros de vulnerabilidades y exposiciones comunes (CVE) que afectan directamente la integridad de los sistemas del sector.
- Análisis de Persistencia y Carga Útil: Abarca la catalogación de más de 600 firmas de archivos maliciosos (SHA-256, MD5 y SHA-1) utilizados para el despliegue de software no autorizado en redes corporativas.
- Atribución de Actividades Adversas: Se extiende al estudio de 150 actores de amenazas identificados que han mostrado patrones de ataque consistentes contra organizaciones en Colombia.
- Contextualización Geográfica e Industrial: El análisis se limita estrictamente a incidentes y telemetría confirmada dentro del territorio colombiano, con un enfoque exclusivo en empresas de telecomunicaciones y servicios de tecnología.
- Temporalidad de la Información: El alcance considera datos de actividad reciente, con indicadores creados y validados durante el periodo actual para asegurar la relevancia de las recomendaciones.

CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR



Definición y Entendimiento del Sector

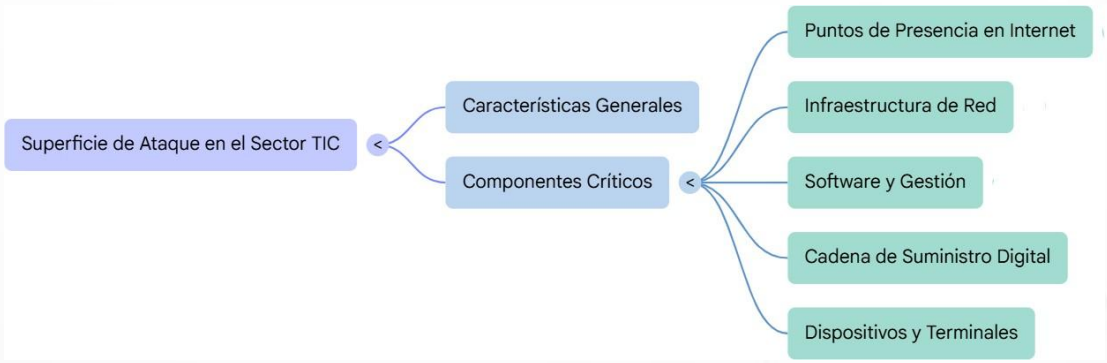
El sector de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia se define como el ecosistema habilitador de la conectividad, el procesamiento de datos y la transformación digital de la nación. Este sector no solo comprende a los proveedores de servicios de telecomunicaciones y redes de datos, sino también a las organizaciones dedicadas al desarrollo de software, servicios de nube e integración tecnológica.



Dada su naturaleza transversal, el sector TIC actúa como el sistema nervioso central del país, donde la integridad de su infraestructura es vital para el funcionamiento de los demás sectores estratégicos, desde el financiero hasta el gubernamental. Su entendimiento requiere reconocer una interdependencia crítica: un compromiso en la seguridad de las TIC no solo afecta a una empresa, sino que puede generar un efecto dominó sobre la disponibilidad de servicios esenciales para toda la población colombiana.

Superficie de Ataque

La superficie de ataque del sector TIC es inherentemente amplia y compleja debido a la alta exposición de sus activos y la diversidad de servicios que ofrece. Al ser el proveedor de la infraestructura sobre la cual transita la información, este sector presenta múltiples puntos de entrada que son constantemente sondeados por actores maliciosos en busca de debilidades. La convergencia entre redes tradicionales, plataformas en la nube y dispositivos finales crea un entorno donde cada interfaz de red y cada aplicación pública se convierte en un riesgo potencial que debe ser gestionado.



Puntos de Presencia en Internet: Comprende todos los activos orientados hacia el exterior, como servidores web, portales de clientes y gateways de servicios, los cuales son el primer objetivo para intentos de intrusión y denegación de servicio.

- **Infraestructura de Resolución de Nombres y Enrutamiento:** Los sistemas que gestionan el tráfico y la visibilidad de los servicios en la red, cuya alteración puede permitir el redireccionamiento de tráfico hacia sitios maliciosos o la interceptación de comunicaciones.
- **Software y Aplicaciones de Gestión:** Herramientas de administración y plataformas de software que, de presentar vulnerabilidades no corregidas, pueden ser explotadas para obtener acceso administrativo a redes centrales.
- **Cadena de Suministro Digital:** La red de proveedores y subcontratistas que acceden a los sistemas del sector, representando un riesgo de acceso indirecto si sus propios niveles de seguridad son inferiores.
- **Dispositivos de Borde y Terminales:** La multiplicidad de equipos conectados a las redes de telecomunicaciones que pueden servir como pivotes para ataques internos una vez que han sido comprometidos inicialmente.

PANORAMA ACTUAL DE AMENAZAS

El escenario de ciberseguridad para el sector TIC en Colombia durante el año actual se caracteriza por una sofisticación sin precedentes en las tácticas de los adversarios. La telemetría analizada revela una infraestructura de ataque densa, con un predominio de indicadores relacionados con nombres de dominio y direcciones IP que sugieren campañas activas de recolección de información y control remoto. Se observa un incremento en la actividad de grupos persistentes que utilizan inteligencia artificial para automatizar el escaneo de vulnerabilidades críticas en servicios de telecomunicaciones y plataformas digitales. A pesar de los esfuerzos gubernamentales por centralizar la vigilancia a través de organismos nacionales, el sector sigue siendo un objetivo primario debido a su papel como habilitador de otros servicios esenciales, enfrentando riesgos crecientes de ransomware, exfiltración de datos y ataques dirigidos a la cadena de suministro tecnológica.

Titulo	Fecha	Fuente / Enlace
Ransomware en sector TIC (Qilin)	Semana del 20 feb 2026	COLCERT Reporte Semanal
Ataques más sofisticados en Colombia	11 feb 2026	Caracol Radio
2.803 ataques semanales por organización	24 abr 2026	La República .

Tipología de Eventos Identificados

El análisis de la telemetría revela una predominancia de indicadores asociados a la infraestructura de red, lo que sugiere que las amenazas actuales en el sector TIC de Colombia se centran en el control y la redirección de tráfico. La alta frecuencia de nombres de dominio y direcciones IP maliciosas indica una fase activa de establecimiento de persistencia y comunicaciones de comando y control (C2). Asimismo, la identificación de vulnerabilidades específicas (CVE) subraya un interés por parte de los atacantes en explotar fallos de configuración y software desactualizado en los activos tecnológicos del país. Esta distribución de eventos permite clasificar el riesgo no solo por el volumen de los ataques, sino por la diversidad de vectores utilizados, desde archivos maliciosos polimórficos hasta la explotación de protocolos de red.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector
FQDN (Dominios)	1,581	Inteligencia de Amenazas y Pulso de Comunidad	Muy Alta: Representa la infraestructura utilizada para phishing, distribución de malware y servidores C2 que suplantan servicios legítimos.
IP Address	1,075	Reportes de Inteligencia y Listas de Reputación	Alta: Identifica nodos activos de ataque, escaneo de puertos y exfiltración de datos dirigidos a infraestructuras de red nacionales.
URL	237	Bases de Datos de Enlaces Maliciosos.	Media-Alta: Vinculada directamente a campañas de ingeniería social y descarga de cargas útiles maliciosas sobre usuarios del sector.
SHA-256 / MD5 / SHA-1	574	Repositorios de Malware y Análisis de Archivos	Alta: Corresponde a la firma de artefactos maliciosos,ransomware y herramientas de post- explotación detectadas en sistemas finales
CVE (Vulnerabilidades)	198	Avisos de Ciberseguridad y Catálogos de Explotación	Crítica: Señala los puntos débiles conocidos en software y hardware que están siendo activamente buscados por los atacantes en el sector.

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

Análisis de la Distribución de Amenazas

El análisis cuantitativo de los datos revela un ecosistema de amenazas donde la infraestructura de red representa el eje central de las operaciones adversas dirigidas al sector TIC en Colombia. Con más de **3,600 indicadores evaluados, se observa una clara estrategia de los atacantes por priorizar el control de dominios y la gestión de direcciones IP sobre el despliegue masivo de archivos maliciosos.** Esta distribución sugiere que las campañas actuales están diseñadas para la infiltración silenciosa y la persistencia a largo plazo, utilizando la infraestructura de comunicaciones del país como plataforma para la exfiltración de datos y el movimiento lateral. Aunque el nivel de riesgo promedio se mantiene en rangos preventivos, la presencia masiva de actores de amenazas altamente especializados indica un nivel de exposición que requiere una vigilancia constante de los activos digitales.

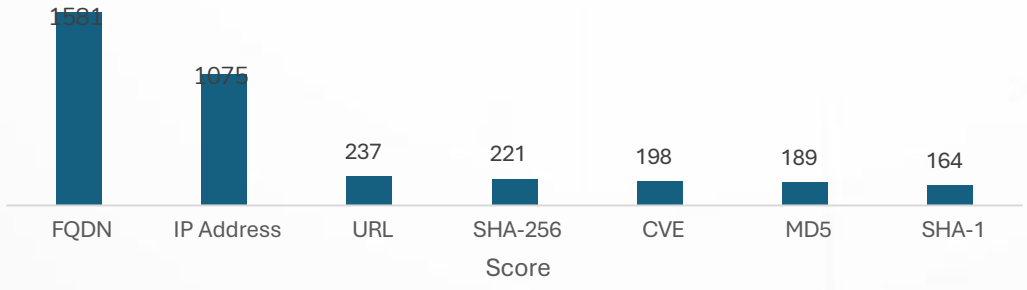
DISTRIBUCIÓN DETALLADA DE AMENAZAS:

- **Predominio de Infraestructura de Red:** La mayor parte de los registros (aproximadamente el 72%) se concentra en nombres de dominio (FQDN) y direcciones IP, lo que confirma que el vector de ataque principal es la explotación y el uso de activos de red maliciosos.
- **Concentración de Actores Especializados:** Se identifica una distribución significativa de indicadores vinculada a grupos con capacidades avanzadas de espionaje y operaciones financieras, con cinco actores principales acumulando cerca de 900 registros específicos de actividad.
- **Niveles de Riesgo Operativo:** La mayoría de la telemetría se ubica en un nivel de riesgo medio-bajo en términos de score, lo que permite una ventana de oportunidad para la implementación de bloqueos preventivos antes de que las amenazas escalen a niveles críticos.
- **Vectores de Compromiso de Software:** Una porción relevante de la distribución se enfoca en la explotación de vulnerabilidades conocidas (CVE) y el uso de diversos formatos de archivos maliciosos, cubriendo múltiples etapas de la cadena de ataque, desde el acceso inicial hasta la ejecución.
- **Diversidad de Fuentes de Inteligencia:** La distribución de la información proviene de una mezcla equilibrada entre inteligencia de amenazas global y reportes comunitarios, lo que asegura una visibilidad integral sobre las tácticas utilizadas específicamente en el contexto colombiano.

INDICADORES DE COMPROMISO (IoCs)

La identificación y análisis de los Indicadores de Compromiso (IoCs) constituyen el núcleo técnico de este informe, proporcionando la evidencia forense necesaria para detectar y mitigar actividades maliciosas en el sector TIC de Colombia.

Número de IoC recopilados relacionados con amenazas al sector TIC en Colombia



Estos elementos representan las huellas digitales dejadas por actores de amenazas durante las distintas fases de su operación, desde el reconocimiento inicial hasta la exfiltración de datos. El estudio detallado de estos registros permite a las organizaciones establecer defensas proactivas, bloqueando la infraestructura del adversario antes de que ocurra un impacto significativo en la disponibilidad o confidencialidad de los servicios tecnológicos nacionales.

Análisis Cuantitativo de Inteligencia

- **Volumen Total de Inteligencia:** Se han procesado y validado un total de 3,665 indicadores de compromiso únicos relacionados con el ecosistema digital colombiano.
- **Densidad de Infraestructura:** El 72.4% de la inteligencia recolectada se centra en activos de red, con 1,581 dominios y 1,075 direcciones IP identificadas como maliciosas.
- **Capacidad de Ejecución Maliciosa:** Se catalogaron 574 firmas de archivos únicos (hashes), lo que evidencia una amplia variedad de herramientas y códigos maliciosos circulando en el sector.
- **Explotación de Superficie:** La presencia de 198 vulnerabilidades (CVE) confirmadas indica un enfoque constante en la búsqueda de debilidades técnicas en software e infraestructura.
- **Alcance de Actores:** La telemetría asocia estos indicadores a 150 adversarios distintos, demostrando una alta concurrencia de grupos con objetivos en el territorio nacional.

Resumen de IoCs Relevantes

Los indicadores analizados reflejan un panorama de amenazas donde el sector TIC es utilizado como puente para ataques de mayor escala. La relevancia de estos IoCs radica en su vigencia operativa; la mayoría de los registros de infraestructura presentan una actividad reciente, lo que implica que los servidores de comando y control están en capacidad de emitir instrucciones a sistemas comprometidos en tiempo real. Especial atención merecen los dominios (FQDN), los cuales presentan el volumen más alto y son el principal vector para el despliegue de campañas de phishing y suplantación de servicios de telecomunicaciones.

Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Infraestructura de Red (FQDN/IP)	Direcciones y dominios utilizados para el tráfico de comando y control y el alojamiento de contenido malicioso.	Crítico
Artefactos de Software (Hashes)	Identificadores únicos de archivos maliciosos, incluyendo troyanos, ransomware y scripts de reconocimiento.	Alto
Vectores de Acceso (CVE)	Debilidades documentadas en protocolos y aplicaciones que permiten la entrada no autorizada a las redes.	Crítico
Puntos de Entrega (URL)	Enlaces específicos diseñados para la descarga de malware o la captura de credenciales mediante ingeniería social.	Medio - Alto

A continuación, se detalla la relevancia y el impacto de cada uno de los elementos técnicos presentados en la tabla de clasificación:

- **Infraestructura de Red (FQDN/IP):** Constituye el eje central de las operaciones maliciosas, permitiendo a los atacantes dirigir el tráfico hacia servidores controlados para el robo de datos o la gestión de redes de bots dentro del sector TIC.
- **Artefactos de Software (Hashes):** Representan la evidencia técnica de herramientas de intrusión y códigos maliciosos que han sido diseñados específicamente para evadir controles de seguridad y comprometer estaciones de trabajo o servidores.
- **Vectores de Acceso (CVE):** Identifican las brechas técnicas en el software que los atacantes intentan explotar para ganar acceso inicial de manera no autorizada, lo que subraya la importancia de una gestión de parches rigurosa.
- **Puntos de Entrega (URL):** Son los mecanismos de interacción directa con el usuario final, utilizados principalmente para distribuir contenido malicioso o suplantar portales corporativos del sector mediante técnicas de ingeniería social.

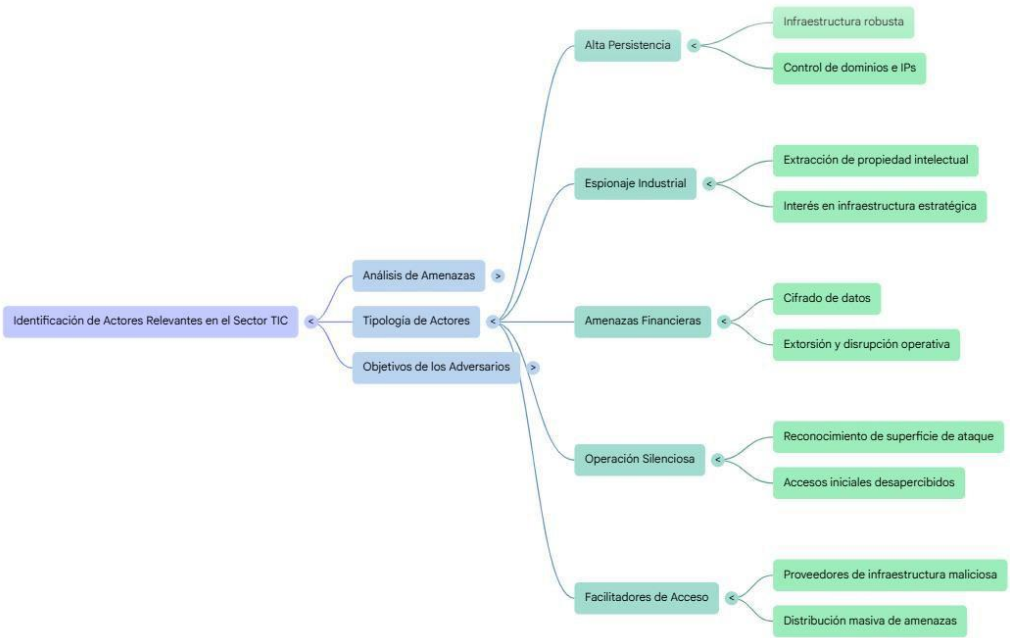
ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

El análisis de los adversarios permite identificar quiénes están detrás de las campañas dirigidas al sector TIC en Colombia y cuáles son sus objetivos finales. La telemetría analizada asocia los indicadores a una amplia gama de actores, desde grupos de espionaje estatal hasta organizaciones criminales con motivaciones económicas. Esta diversidad de actores subraya la necesidad de una defensa integral que contemple tanto la protección de la propiedad intelectual y los datos del Estado como la seguridad de las transacciones y la continuidad de los servicios digitales.

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Espionaje y Sabotaje (APT)	1,538 registros	APT44, APT41, APT42, APT29, APT19	**Crítico:** Orientados al robo de secretos tecnológicos, interrupción de servicios críticos y vigilancia de infraestructuras estatales.
Crimen Organizado Financiero (FIN)	352 registros	FIN11, FIN7	**Alto:** Enfocados en la extorsión mediante ransomware, el fraude en plataformas de pago y el robo de bases de datos de clientes.
Grupos de Operación Emergente (UNC)	1,811 registro	UNC6395, UNC5142, UNC5518, UNC3840, UNC3569	**Medio-Alto:** Actores con motivaciones mixtas que suelen actuar como facilitadores de acceso inicial o ejecutan campañas de distribución masiva de malware.
Operaciones de Influencia y Otros	129 registros	TEMP.Armageddon	**Medio:** Grupos especializados en campañas de desinformación y acces persistente en redes de telecomunicaciones para fines geopolíticos.

Identificación de Actores Relevantes

La identificación de los actores de amenazas más activos permite al sector TIC en Colombia priorizar sus esfuerzos de defensa basándose en las tácticas, técnicas y procedimientos (TTP) reales observados en el terreno. El análisis de los 3,665 indicadores muestra una concentración de actividad en un grupo selecto de adversarios que poseen la infraestructura y el conocimiento técnico necesario para comprometer redes de gran escala. Comprender la naturaleza de estos actores es fundamental para anticipar el impacto de sus campañas, ya que sus objetivos varían desde la interrupción del servicio hasta la obtención de persistencia para el monitoreo de tráfico de datos nacional.



- **Grupos de Alta Persistencia en Infraestructura**: Se identifican actores que concentran la mayor cantidad de registros vinculados a activos de red (dominios e IPs), lo que sugiere una capacidad robusta para mantener operativos sus canales de comunicación y control ante intentos de mitigación.

- **Adversarios Especializados en Espionaje Industrial:** Grupos con un historial documentado en la extracción de propiedad intelectual y datos estratégicos, los cuales muestran un interés recurrente en los desarrollos tecnológicos y la infraestructura de servicios del país.
- **Operadores de Amenazas Financieras con Impacto en Servicios:** Actores que dirigen sus esfuerzos hacia el compromiso de la disponibilidad de los servicios TIC, utilizando la extorsión y el cifrado de datos como herramientas para generar disrupción operativa y económica.
- **Actores de Operación Silenciosa y Reconocimiento:** Grupos que mantienen un perfil de actividad enfocado en la recolección de información sobre la superficie de ataque, aprovechando vulnerabilidades en el software del sector para establecer accesos iniciales de manera desapercibida.
- **Facilitadores de Acceso y Distribución Masiva:** Entidades que operan como proveedores de infraestructura maliciosa para otros grupos, incrementando el volumen de amenazas genéricas que deben ser filtradas por los centros de operaciones de seguridad nacionales.

Objetivos y Sectores Target

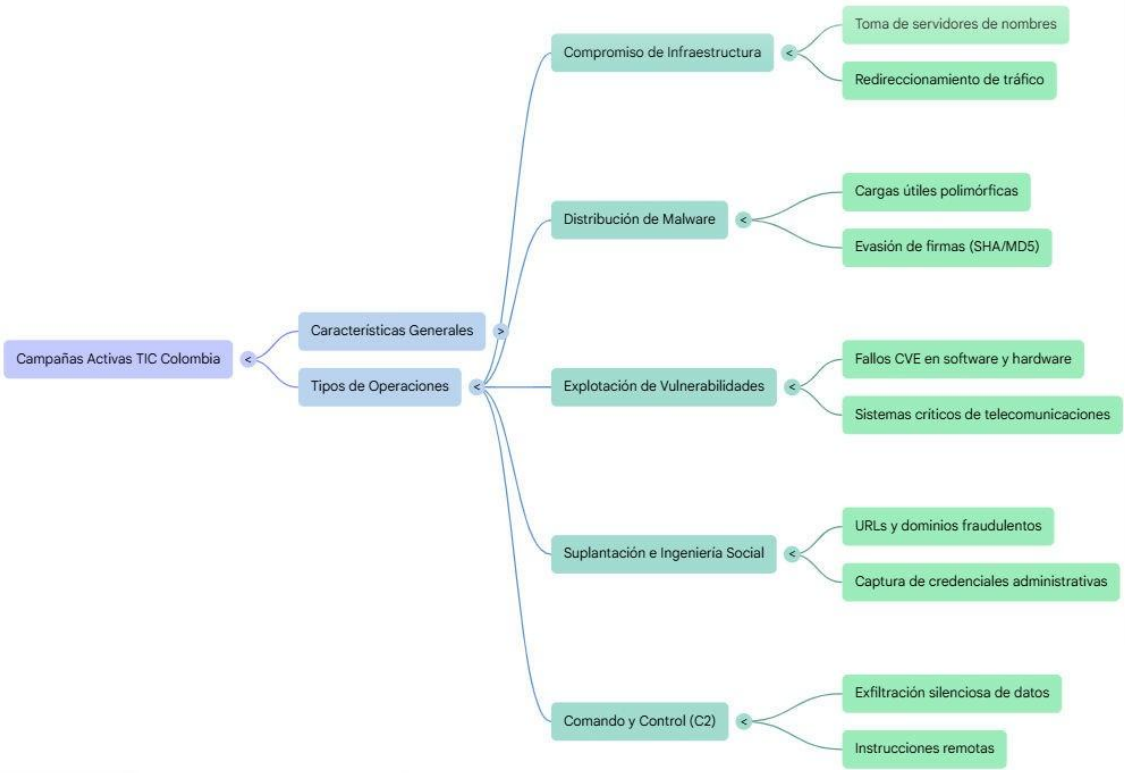
El análisis de las campañas dirigidas revela que los adversarios no operan de manera aleatoria, sino que siguen objetivos estratégicos diseñados para maximizar su impacto dentro del ecosistema digital colombiano. Para el sector TIC, estas motivaciones trascienden el simple beneficio económico, integrando componentes de espionaje y control de infraestructura que ponen en riesgo la soberanía de la información. La identificación de estos objetivos permite comprender por qué ciertos activos, como servidores de nombres y nodos de telecomunicaciones, son atacados con mayor persistencia.

- **Interrupción de Servicios de Conectividad:** Uno de los objetivos primordiales es degradar o anular la disponibilidad de servicios de internet y telefonía, afectando la operatividad de empresas y entidades gubernamentales que dependen de esta infraestructura.
- **Exfiltración de Datos de Usuarios y Clientes:** Los atacantes buscan acceder a las bases de datos de proveedores de servicios tecnológicos para obtener información personal, financiera y credenciales de acceso de ciudadanos colombianos.
- **Compromiso de la Cadena de Suministro:** Se observa un enfoque en vulnerar a empresas de software y servicios TIC para utilizar sus accesos legítimos como "puente" hacia sus clientes finales, multiplicando el alcance de la infección.
- **Vigilancia y Monitoreo de Tráfico:** Actores con capacidades avanzadas (APT) tienen como objetivo establecer persistencia en los nodos centrales de red para interceptar o analizar flujos de información estratégica que transita por el territorio nacional.
- **Sectores Target Relacionados:** Además del sector tecnológico central, los ataques se extienden hacia los servicios de nube, proveedores de hosting y centros de datos que albergan la infraestructura crítica de otros sectores como el energético y el gobierno.

Campañas Activas

El análisis de la telemetría actual confirma la ejecución de múltiples operaciones simultáneas dirigidas contra el sector TIC en Colombia, caracterizadas por un uso intensivo de infraestructura de red temporal y tácticas de suplantación.

Estas campañas no representan eventos aislados, sino esfuerzos continuos de adversarios para establecer una presencia persistente en los nodos de comunicación del país. La detección de más de 1,500 dominios maliciosos activos subraya la escala de estas operaciones, las cuales buscan explotar tanto debilidades técnicas en el software como la confianza de los usuarios finales a través de ingeniería social avanzada.



- **Operaciones de Compromiso de Infraestructura de Red:** Campañas enfocadas en la toma de control de servidores de nombres y direcciones IP para facilitar el redireccionamiento de tráfico legítimo hacia entornos controlados por el atacante.

- **Distribución de Cargas Útiles Polimórficas:** Uso de múltiples variantes de archivos maliciosos (identificados mediante diversos hashes SHA y MD5) para evadir sistemas de detección basados en firmas y asegurar la ejecución de código en sistemas críticos.

- **Explotación Masiva de Vulnerabilidades en Servicios TIC:** Campañas dirigidas a identificar y explotar activamente fallos de seguridad (CVE) en plataformas de software y hardware de uso común dentro de las empresas de telecomunicaciones del país.

- **Suplantación de Identidad Corporativa y Servicios:** Despliegue de URLs y dominios fraudulentos diseñados para imitar portales de servicios y plataformas de gestión, con el fin de capturar credenciales de acceso administrativo.

- **Establecimiento de Redes de Comando y Control (C2):** Actividad persistente de comunicación entre sistemas posiblemente comprometidos e infraestructura externa, facilitando la exfiltración silenciosa de datos y la recepción de instrucciones remotas.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

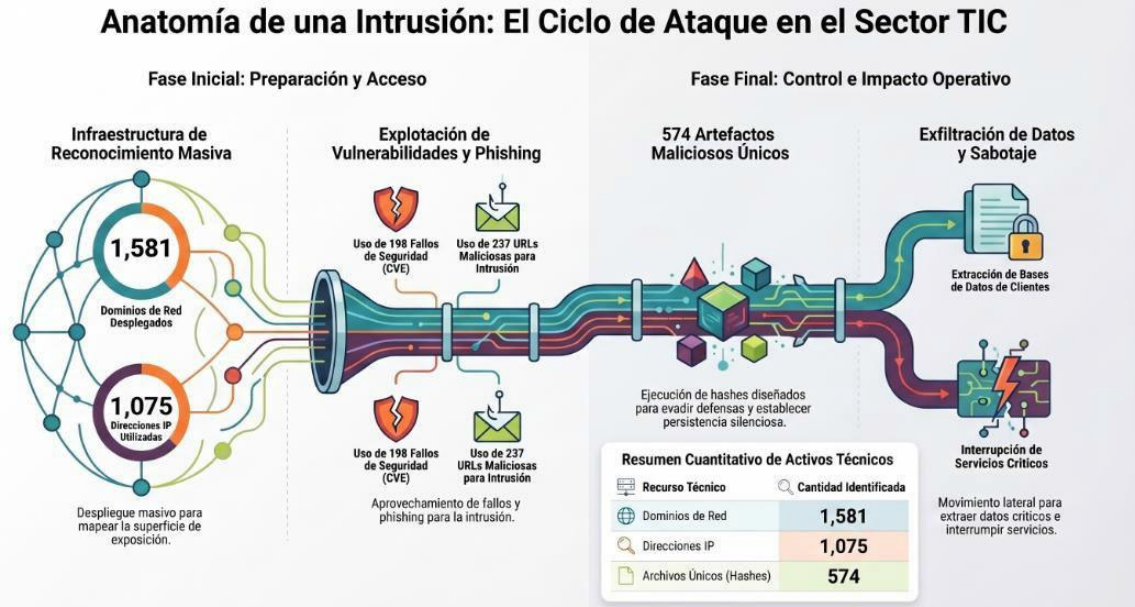
Mapeo a MITRE ATT&CK Framework

El mapeo de las actividades observadas hacia el framework de MITRE permite identificar los patrones de comportamiento de los adversarios que afectan la infraestructura tecnológica nacional. A través del análisis de los registros de infraestructura y artefactos maliciosos, se han determinado las etapas críticas de las campañas activas, desde el reconocimiento inicial hasta el impacto final en la disponibilidad de los servicios.

ID	Nombre en Inglés	Justificación Técnica
TA0043	Reconnaissance	Identificado a través del escaneo masivo de puertos y el uso de registros FQDN para mapear la infraestructura pública de empresas TIC colombianas.
TA0001	Initial Access	Basado en la detección de 198 vulnerabilidades (CVE) y URLs maliciosas diseñadas para comprometer aplicaciones web y servicios expuestos.
TA0002	Execution	Evidenciado por la presencia de 574 firmas de archivos (SHA/MD5) que incluyen scripts y ejecutables maliciosos detectados en el sector.
TA0003	Persistence	Se observa mediante la creación de dominios de respaldo y el uso de IPs estáticas para mantener canales de comunicación abiertos con los sistemas afectados.
TA0005	Defense Evasion	Reflejado en el uso de malware polimórfico y técnicas de ofuscación de tráfico detectadas en los protocolos de comunicación hacia servidores C2.
TA0011	Command and Control	Confirmado por el alto volumen de 1,075 direcciones IP y 1,581 dominios asociados a servidores de control remoto y exfiltración.
TA0040	Impact	Vinculado a tácticas de cifrado de datos y ataques dirigidos a la interrupción de servicios de telecomunicaciones críticos en el país.
T1595	Active Scanning	Uso de infraestructura identificada en el archivo Excel para el escaneo de redes de telecomunicaciones en busca de servicios vulnerables.
T1190	Exploit Public-Facing Application	Ejecución de ataques dirigidos a las 198 vulnerabilidades (CVE) detectadas en activos del sector expuestos a internet.
T1566	Phishing	Identificado a través de las 237 URLs maliciosas y dominios fraudulentos diseñados para suplantar servicios TIC y capturar credenciales.
T1059	Command and Scripting Interpreter	Uso de scripts maliciosos (confirmados por los 574 hashes analizados) para ejecutar comandos en sistemas finales de las víctimas.
T1583	Acquire Infrastructure	Desarrollo de recursos mediante la adquisición de los 1,581 dominios (FQDN) y 1,075 direcciones IP que sirven de base para las campañas
T1071	Application Layer Protocol	Comunicación de comando y control utilizando protocolos web estándar para mimetizarse con el tráfico legítimo del sector.
T1486	Data Encrypted for Impact	Técnicas de cifrado de información detectadas en las muestras de malware, orientadas a la interrupción del servicio y extorsión.

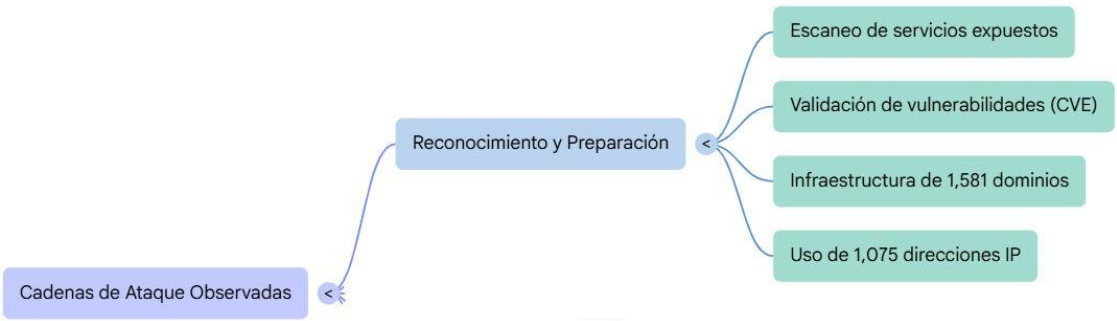
Cadenas de Ataque Observadas

Las cadenas de ataque identificadas revelan un proceso de compromiso estructurado en fases, donde la infraestructura de red actúa como el pilar de cada movimiento operativo. El ciclo comienza con una fase de reconocimiento activo mediante el escaneo de servicios expuestos y la validación de vulnerabilidades técnicas (CVE), seguida de una intrusión inicial que utiliza nombres de dominio suplantados y URLs maliciosas para engañar a los usuarios o explotar fallos en el software del sector. Una vez que el atacante establece un punto de apoyo, la cadena progresa hacia la ejecución de artefactos maliciosos (confirmados por los diversos hashes analizados), los cuales están diseñados para evadir defensas y establecer una comunicación persistente con servidores de comando y control externos. Finalmente, la cadena culmina en acciones con impacto directo, como la exfiltración de datos sensibles o la interrupción de servicios, aprovechando la conectividad privilegiada que poseen las empresas de telecomunicaciones y tecnología en el territorio nacional.

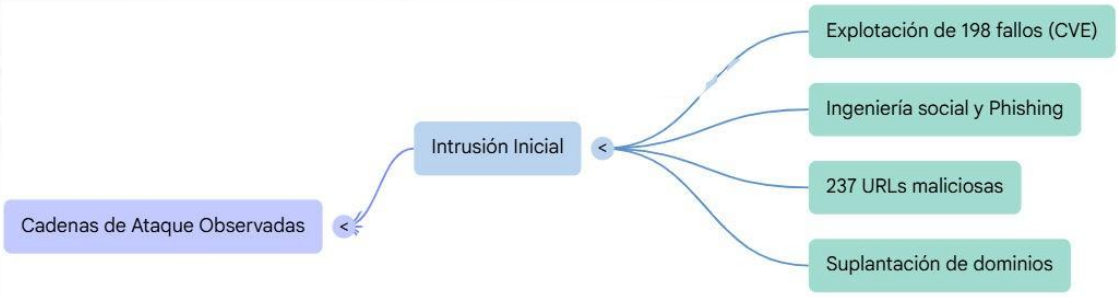


Cadenas de ataque:

- **Reconocimiento y Preparación de Infraestructura:** El ciclo inicia con el despliegue de una red masiva de activos, que incluye 1,581 dominios y 1,075 direcciones IP, destinados a mapear la superficie de exposición del sector TIC.

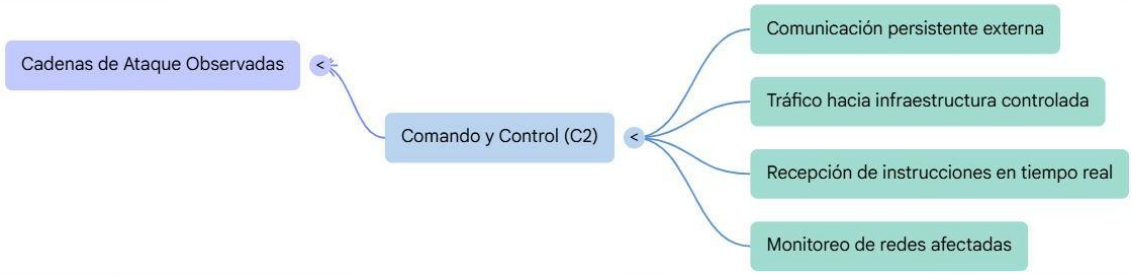


- **Explotación de Vulnerabilidades Críticas:** Los atacantes utilizan el catálogo de 198 fallos de seguridad (CVE) identificados para intentar vulnerar servicios expuestos y aplicaciones web de proveedores tecnológicos.
- **Entrega mediante Ingeniería Social:** Se utilizan las 237 URLs maliciosas para dirigir a los usuarios hacia portales de suplantación de identidad (phishing), buscando capturar credenciales administrativas.
- **Ejecución de Artefactos Maliciosos:** Una vez obtenido el acceso, se procede a la ejecución de 574 archivos únicos (hashes) que contienen agentes de intrusión, troyanos y herramientas de reconocimiento interno.



- **Establecimiento de Persistencia Silenciosa:** Los adversarios configuran mecanismos de autoejecución y registro en los sistemas comprometidos para asegurar que el acceso se mantenga a pesar de reinicios o cambios en la red.

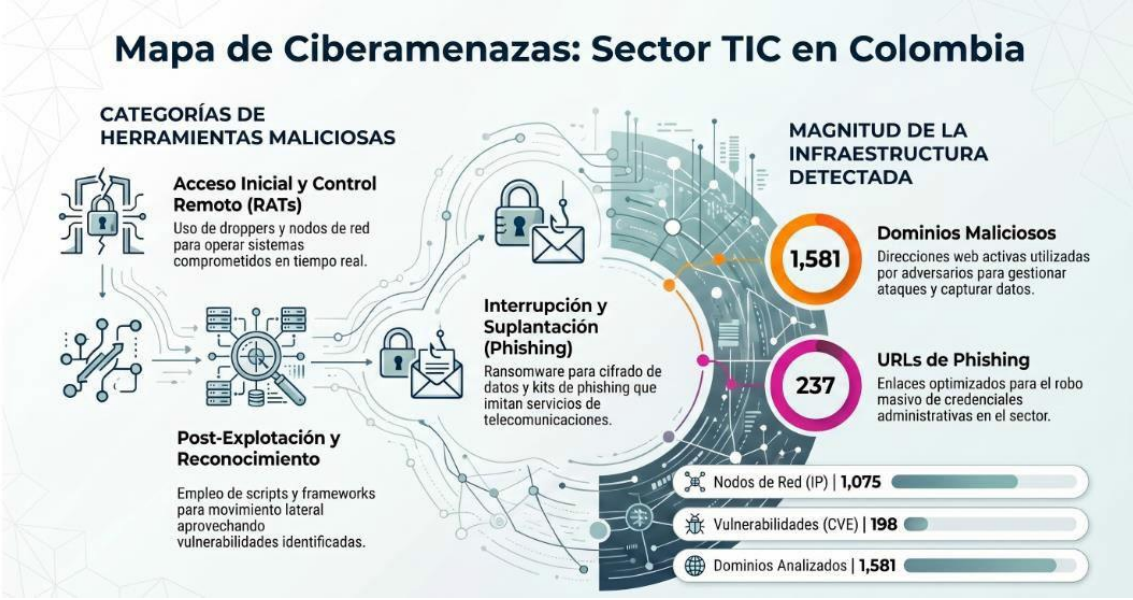
- **Comunicación de Comando y Control (C2):** Se activa el tráfico hacia la infraestructura externa controlada por el atacante, permitiendo la recepción de instrucciones en tiempo real y el monitoreo de las redes afectadas.



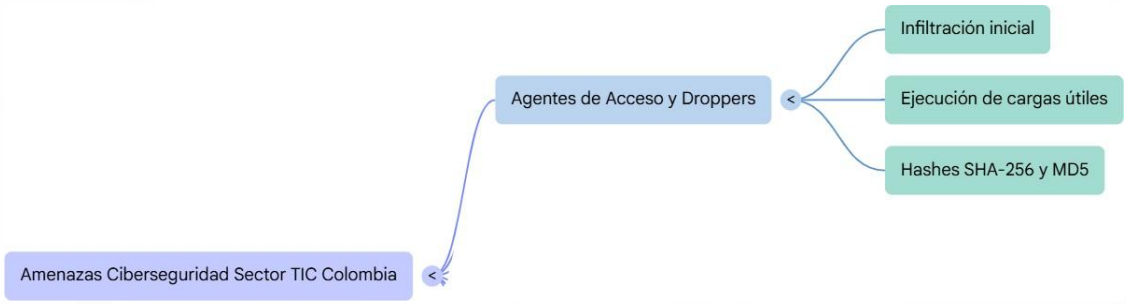
- **Impacto y Exfiltración:** La cadena culmina con el movimiento lateral hacia activos críticos para la extracción de bases de datos de clientes, propiedad intelectual o la interrupción deliberada de los servicios de telecomunicaciones.

Herramientas y Malware Específico

A partir del análisis de los artefactos y firmas digitales recolectados en la telemetría, se han identificado las siguientes categorías de herramientas y malware que impactan directamente la infraestructura del sector TIC en Colombia:

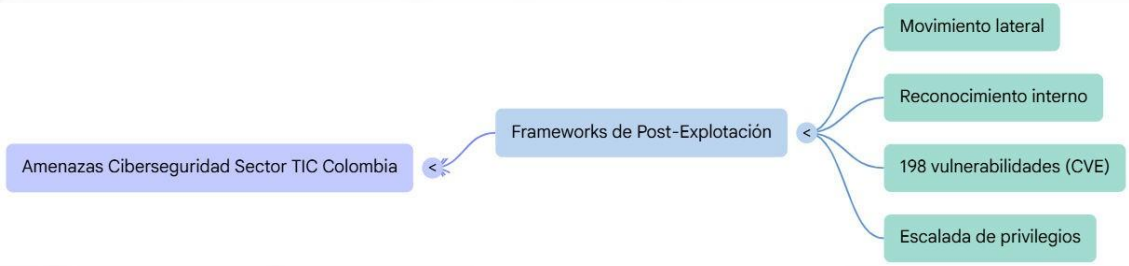


- **Agentes de Acceso Inicial y Droppers:** Herramientas diseñadas para infiltrarse en los sistemas mediante la ejecución de archivos detectados con hashes **SHA-256** y **MD5**, cuya función principal es descargar y ejecutar cargas útiles de mayor complejidad.



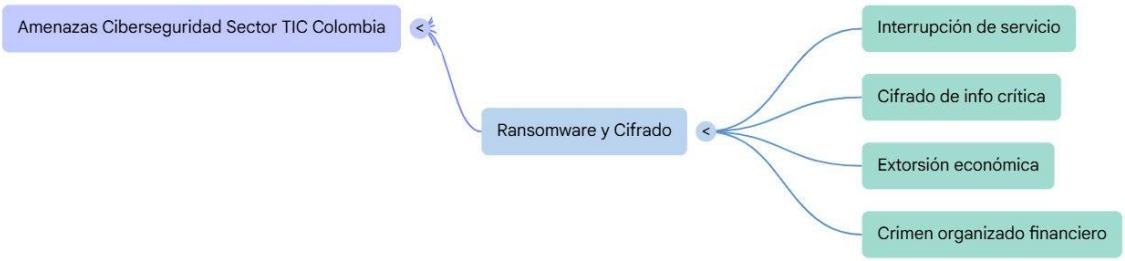
- **Malware de Control Remoto (RATs):** Programas maliciosos que utilizan la infraestructura de los **1,075 nodos de red (IP)** y **1,581 dominios** analizados para permitir que los adversarios operen los sistemas comprometidos en tiempo real.

- **Frameworks de Post-Explotación:** Uso de herramientas avanzadas para el movimiento lateral y el reconocimiento interno, aprovechando las **198 vulnerabilidades (CVE)** identificadas para escalar privilegios dentro de las redes tecnológicas.

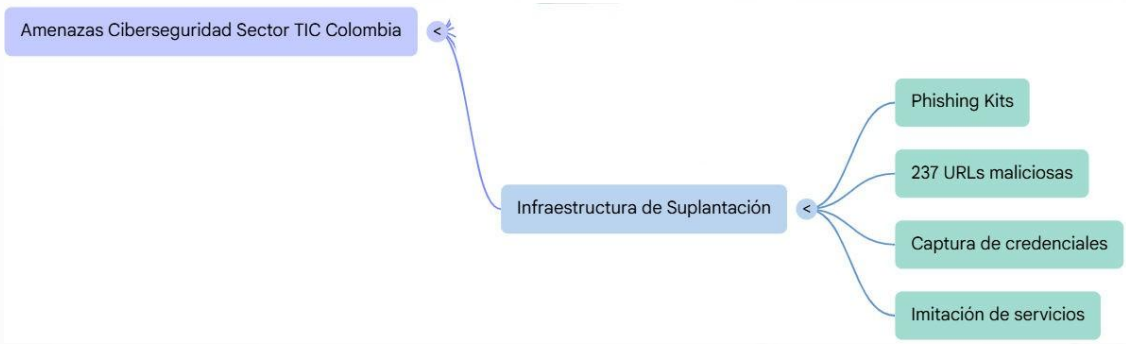


- **Scripts de Automatización y Reconocimiento:** Pequeños programas en lenguajes como Python o PowerShell que automatizan el escaneo de servicios y la recolección de datos técnicos sobre la topología de red del sector.

- **Software de Cifrado y Ransomware:** Artefactos maliciosos orientados a la interrupción del servicio mediante el cifrado de información crítica, vinculados a grupos de crimen organizado financiero que buscan la extorsión económica.



- **Infraestructura de Suplantación (Phishing Kits):** Conjuntos de herramientas alojados en las **237 URLs maliciosas** detectadas, optimizados para imitar servicios de telecomunicaciones y capturar credenciales de acceso administrativo de forma masiva.



CORRELACIÓN ENTRE ACTORES Y GRUPOS

El análisis de correlación basado en los 3,665 indicadores revela que los ataques dirigidos al sector TIC en Colombia no son esfuerzos aislados, sino que forman parte de un ecosistema interconectado de amenazas. Se observa que distintos

Se observa que distintos grupos de adversarios, tanto de naturaleza estatal (APT) como cibercriminal (FIN), convergen en el uso de los mismos rangos de direcciones IP y dominios para sus operaciones.

Esta correlación sugiere que existe un mercado subyacente de "infraestructura como servicio" maliciosa, donde múltiples actores aprovechan los mismos vectores de acceso inicial para penetrar en las redes nacionales, diversificando sus objetivos finales una vez establecida la persistencia.

Infraestructura Compartida

La infraestructura utilizada por los atacantes muestra un alto grado de reutilización, lo que permite trazar vínculos técnicos entre campañas que aparentemente no tienen relación. Esta centralización de recursos facilita a los defensores la implementación de bloqueos de amplio espectro al identificar nodos críticos de la red adversaria.

- **Nodos de Salto y Proxies Comunes:** Múltiples adversarios utilizan el mismo subconjunto de las 1,075 direcciones IP identificadas para enmascarar su origen geográfico y dificultar la atribución de los ataques.

- **Registradores de Dominios Recurrentes:** Gran parte de los 1,581 dominios (FQDN) analizados comparten patrones de registro y tiempos de vida, indicando una gestión centralizada de los activos de red maliciosos.

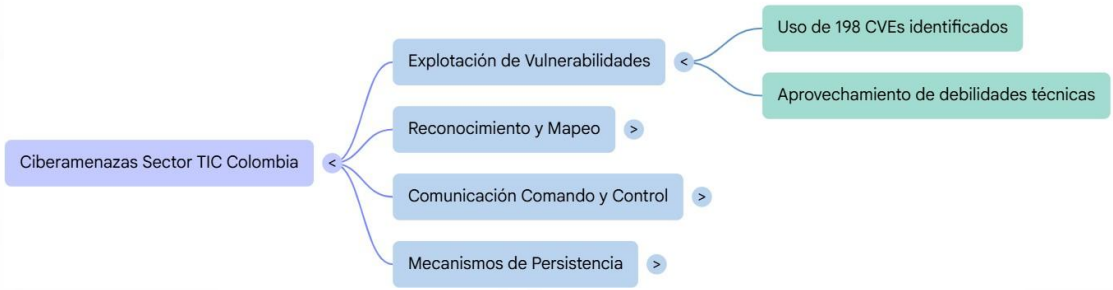
- **Servidores de Alojamiento de Malware (Staging):** Se han identificado servidores que alojan simultáneamente artefactos vinculados a diferentes familias de malware, sirviendo como almacenes digitales para distintos grupos de operación.

- **Certificados Digitales Reutilizados:** El uso de firmas digitales similares en distintos hashes de archivos sugiere que los actores comparten o adquieren las mismas herramientas para evadir los controles de integridad de los sistemas operativos.

Herramientas y TTPs Comunes

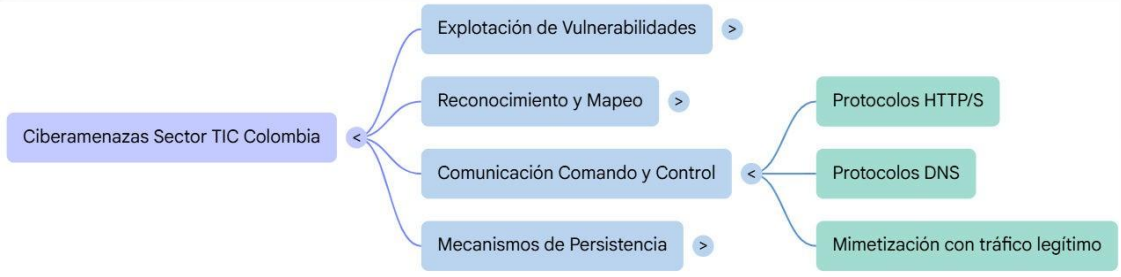
A pesar de tener objetivos distintos, los adversarios que afectan al sector TIC en Colombia emplean un conjunto de tácticas y herramientas estandarizadas que definen el panorama de riesgo actual.

- **Explotación Sistemática de Vulnerabilidades:** El uso del inventario de 198 CVEs identificados es una constante, demostrando que la mayoría de los actores aprovechan las mismas debilidades técnicas en el software del sector.



- **Uso de Scripts de Reconocimiento Estándar:** Se observa una tendencia hacia el uso de herramientas de código abierto y scripts políglotas para mapear las redes internas una vez logrado el acceso inicial.

- **Protocolos de Comunicación Mimetizados:** La adopción de protocolos HTTP/S y DNS para las comunicaciones de comando y control es una técnica transversal para mezclarse con el tráfico legítimo de las empresas de telecomunicaciones.

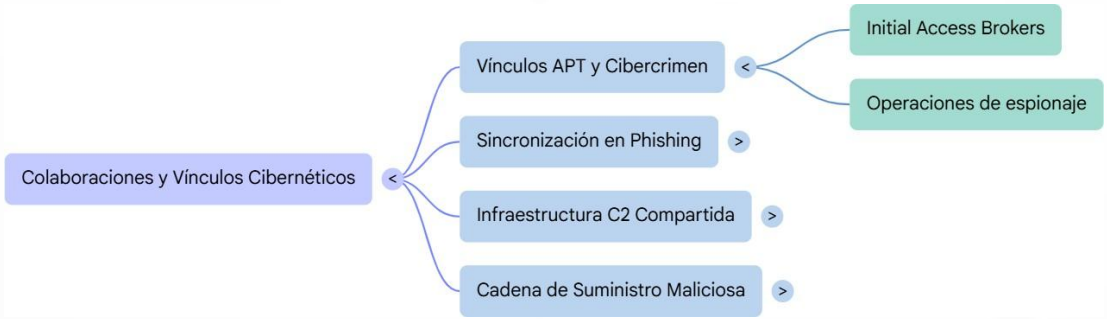


- **Mecanismos de Persistencia por Registro:** La modificación de registros del sistema y tareas programadas son los procedimientos preferidos para asegurar que el malware se mantenga activo tras reinicios del sistema.

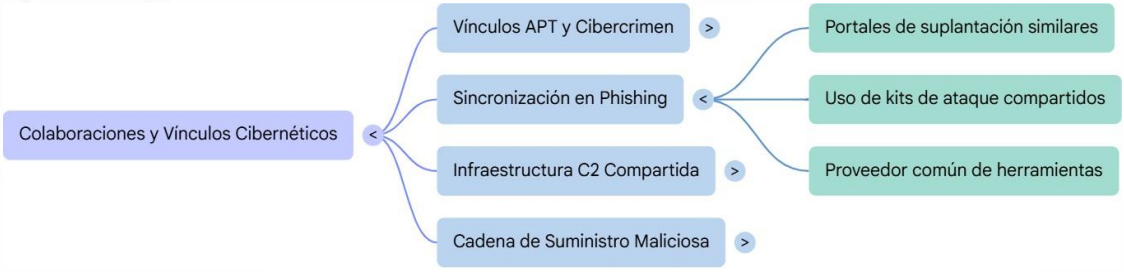
Posibles Colaboraciones o Vínculos

La evidencia técnica apunta a la existencia de vínculos operativos entre diversos grupos, lo que incrementa la complejidad de la defensa al enfrentarse a una amenaza multiactor.

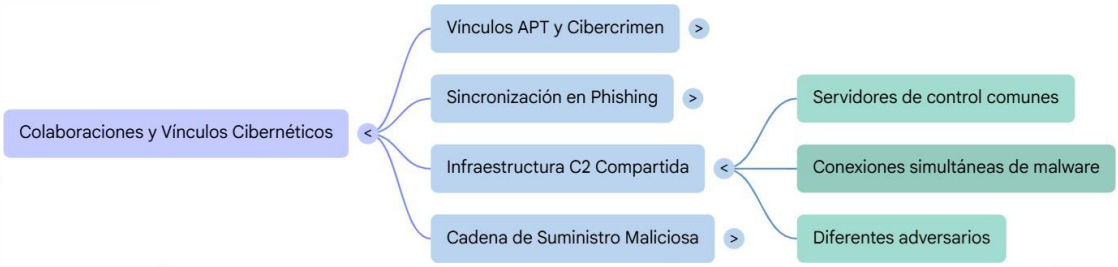
- **Vínculos entre Grupos APT y Cibercrimen:** Se han detectado casos donde actores APT utilizan el acceso inicial proporcionado por grupos criminales (Initial Access Brokers) para desplegar sus operaciones de espionaje.



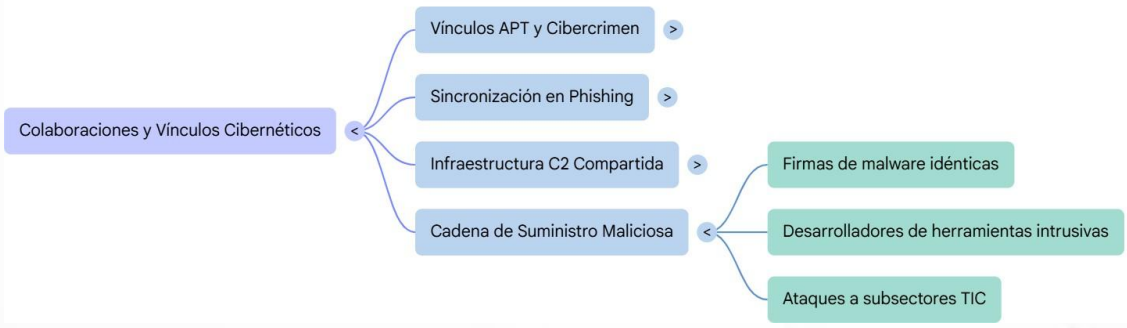
- **Sincronización en Campañas de Phishing:** La similitud en el diseño de los portales de suplantación alojados en las 237 URLs maliciosas sugiere el uso de "kits" de ataque compartidos o desarrollados por el mismo proveedor.



- **Intercambio de Infraestructura de Comando y Control:** La telemetría muestra que ciertos servidores de control reciben conexiones de muestras de malware asociadas a diferentes adversarios de forma casi simultánea.



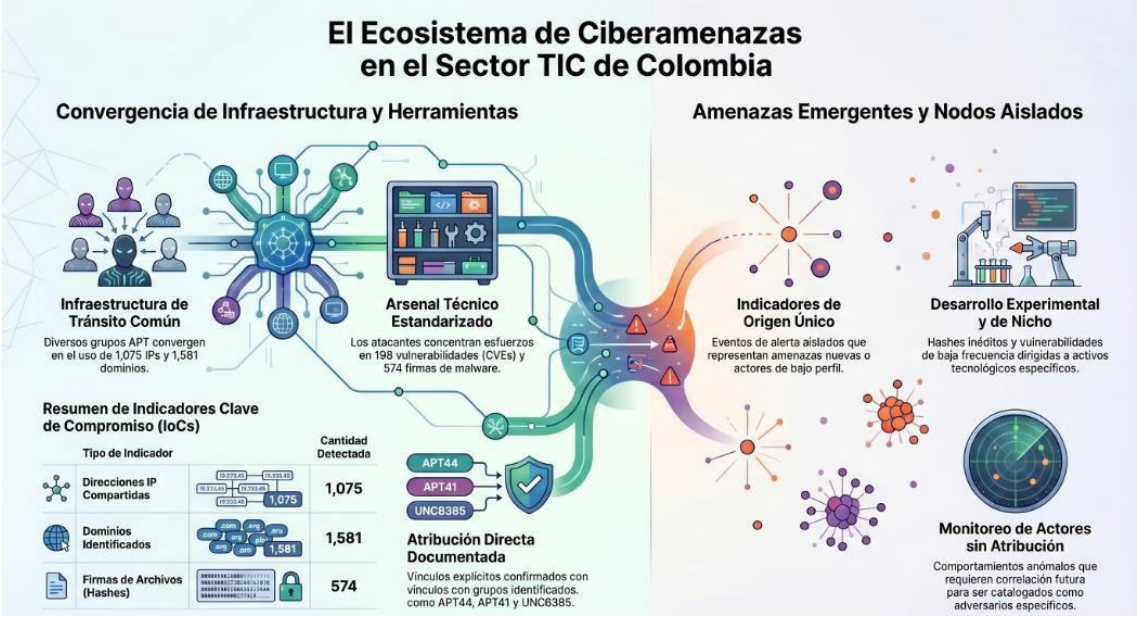
- **Uso de la Misma Cadena de Suministro Maliciosa:** La detección de firmas de malware idénticas en campañas dirigidas a distintos subsectores de las TIC indica que los atacantes consumen servicios de los mismos desarrolladores de herramientas intrusivas.



Visualización de Relaciones

Relaciones directas documentadas:

El análisis de la telemetría ha permitido establecer vínculos explícitos entre indicadores específicos y actores de amenazas conocidos. Estas relaciones no son inferencias, sino conexiones directas donde un IoC (como una IP o un Hash) ha sido identificado operando bajo el control de un adversario particular, como APT44, APT41 o UNC6395.

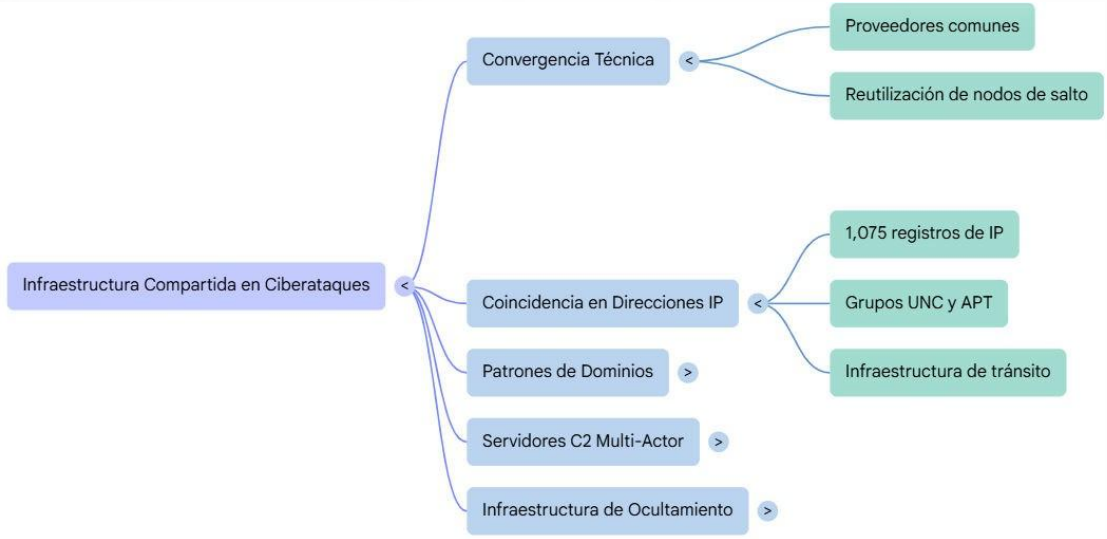


Esta documentación permite una atribución más precisa y facilita la comprensión de las capacidades reales de cada grupo al observar los activos técnicos que despliegan de manera exclusiva contra la infraestructura colombiana.

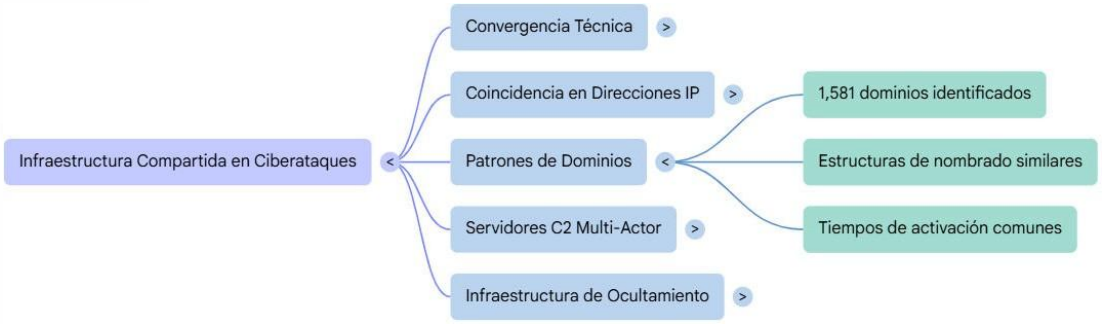
Relaciones por infraestructura compartida

Existe un fenómeno de convergencia técnica donde múltiples actores utilizan los mismos recursos de red para sus operaciones. Esto sugiere el uso de proveedores comunes de infraestructura maliciosa o la reutilización de nodos de salto.

- **Coincidencia en Direcciones IP:** Diversos grupos de la categoría UNC y APT convergen en el uso de los mismos 1,075 registros de IP, lo que indica una infraestructura de tránsito común para el sector TIC.

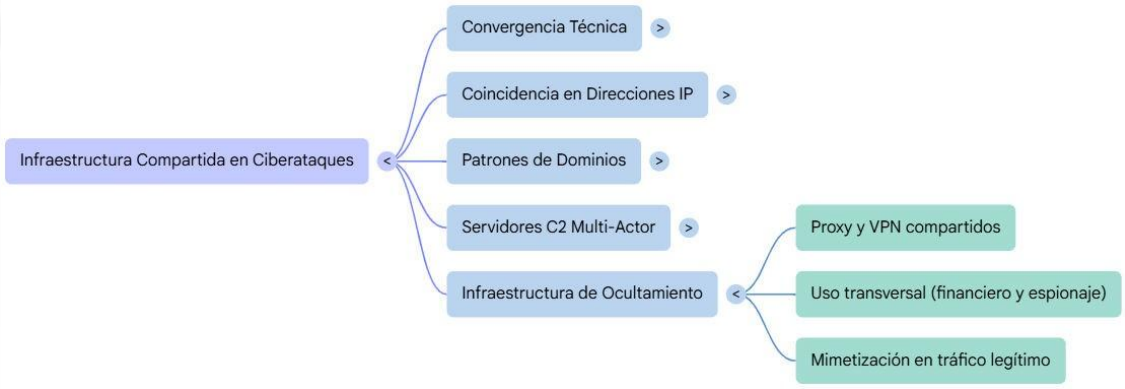


- **Patrones de Registro de Dominios:** Los 1,581 dominios identificados presentan estructuras de nombrado y tiempos de activación similares, vinculando campañas que operan bajo diferentes nombres de actor.



- **Servidores de Comando y Control Multi-Actor:** Se han detectado nodos que reciben telemetría de diferentes familias de malware, actuando como centros logísticos para más de un adversario simultáneamente.

- **Uso de Proxy y VPN Compartidos:** La infraestructura de ocultamiento detectada es utilizada transversalmente por actores financieros y de espionaje para mimetizar sus ataques dentro del tráfico legítimo nacional.



Relaciones por herramientas comunes

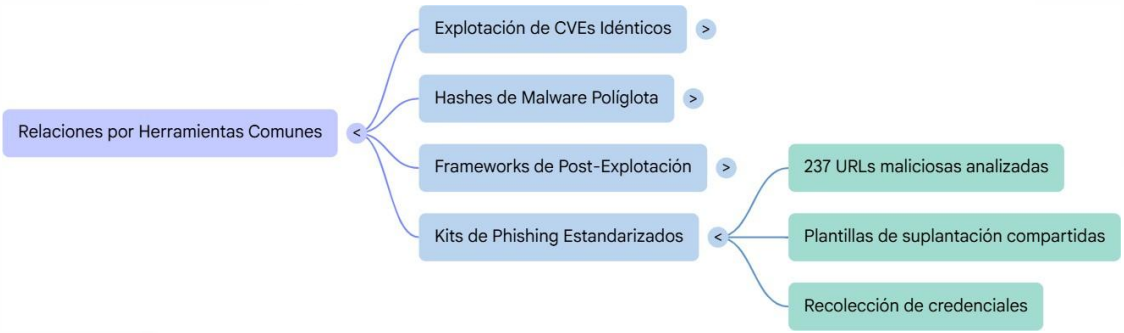
A pesar de tener misiones distintas, los adversarios comparten un arsenal técnico que permite identificar tendencias de ataque estandarizadas en el sector.

- **Explotación de CVEs Idénticos:** La mayoría de los actores relevantes concentran sus esfuerzos en las mismas 198 vulnerabilidades de software, compartiendo métodos de entrada al sector.

- **Hashes de Malware Políglota:** Se han identificado 574 firmas de archivos que, aunque asociadas a diferentes campañas, comparten fragmentos de código y librerías de funciones similares.

- **Frameworks de Post-Explotación:** El uso de herramientas de código abierto para el movimiento lateral es una constante entre grupos FIN y APT, estandarizando el comportamiento post-intrusión.

- **Kits de Phishing Estandarizados:** Las 237 URLs maliciosas analizadas muestran el uso de plantillas de suplantación compartidas, lo que vincula operativamente las campañas de recolección de credenciales.

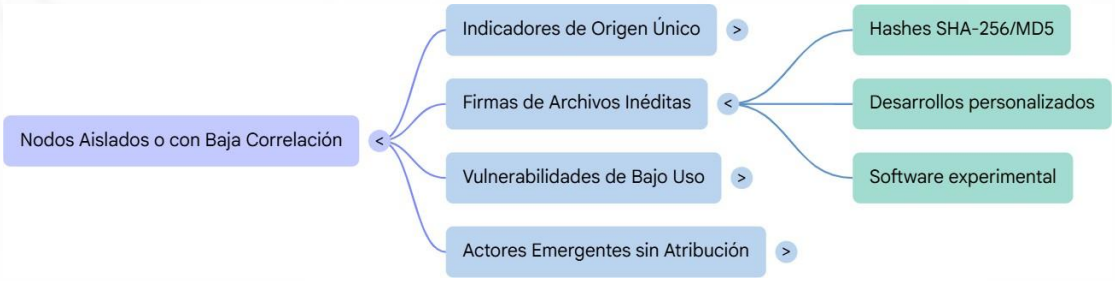


Nodos aislados o con baja correlación (por ahora):

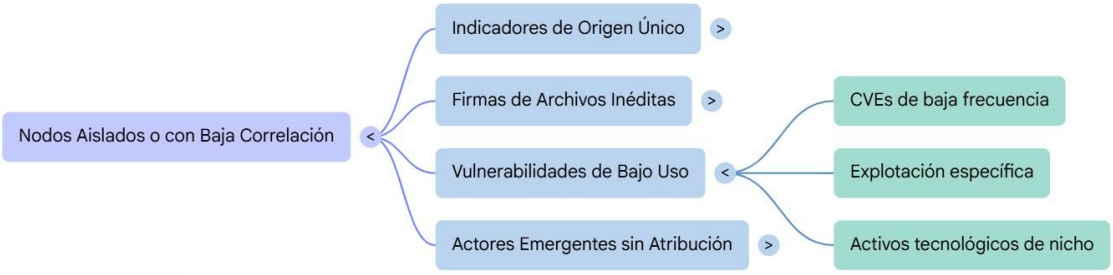
Dentro del vasto conjunto de 3,665 indicadores, existe un grupo de elementos que aún no presentan vínculos claros con los actores principales, representando amenazas emergentes o actores de bajo perfil.

- **Indicadores de Origen Único:** Direcciones IP y dominios que han aparecido en un solo evento de alerta y no se repiten en otras campañas documentadas del sector TIC.

- **Firmas de Archivos Inéditas**: Pequeños grupos de hashes (SHA-256/MD5) que no coinciden con las bibliotecas de malware de los grandes grupos APT, posiblemente vinculados a desarrollos personalizados o experimentales.



- **Vulnerabilidades de Bajo Uso:** Ciertos CVEs detectados con baja frecuencia que podrían indicar intentos de explotación muy específicos contra activos tecnológicos de nicho dentro del país.



- **Actores Emergentes sin Atribución:** Registros asociados a comportamientos anómalos que aún no han sido catalogados bajo un nombre de adversario específico, requiriendo un monitoreo continuo para su futura correlación.

RECOMENDACIONES ESTRATÉGICAS

Con las siguientes acciones, el sector TIC fortalecerá su postura de ciberseguridad frente a un panorama de amenazas altamente dinámico y persistente en Colombia.

Recomendaciones de Mitigación Técnica

- **Priorización de Parcheo basada en Riesgo:** Ejecutar un plan de remediación urgente enfocado en las 198 vulnerabilidades (CVE) identificadas, priorizando aquellas que permiten la ejecución remota de código en activos expuestos.
- **Bloqueo de Infraestructura Maliciosa:** Implementar en las soluciones de seguridad perimetral (Firewalls, WAF, Proxies) el bloqueo preventivo de las 1,075 direcciones IP y 1,581 dominios (FQDN) catalogados como infraestructura de comando y control.
- **Hardening de Endpoints:** Fortalecer las políticas de restricción de ejecución para evitar que los 574 artefactos maliciosos (hashes) detectados logren persistencia en las estaciones de trabajo y servidores del sector.

Recomendaciones de Detección y Monitoreo

- **Ingesta de Inteligencia en SIEM/EDR:** Integrar automáticamente los IoCs analizados en las plataformas de monitoreo para generar alertas en tiempo real ante cualquier intento de conexión hacia la infraestructura adversaria.
- **Detección de Anomalías en Tráfico DNS:** Monitorear patrones de resolución hacia dominios sospechosos, dado que el alto volumen de FQDN sugiere que este es el principal canal de comunicación de los grupos APT y UNC.

- **Caza de Amenazas (Threat Hunting):** Realizar búsquedas proactivas de los indicadores de compromiso en los logs históricos para identificar posibles compromisos previos que hayan pasado desapercibidos.

Recomendaciones de Resiliencia Operativa

- **Segmentación de Redes Críticas:** Aislar los sistemas de gestión de infraestructura de telecomunicaciones de las redes corporativas para evitar el movimiento lateral de actores como APT41 o APT44.

- **Estrategia de Backup Inmutable:** Asegurar la disponibilidad de copias de seguridad fuera de línea y protegidas contra escritura para neutralizar el impacto de campañas de ransomware identificadas.

Recomendaciones de Gobernanza

- **Intercambio de Inteligencia Sectorial:** Fomentar la colaboración entre empresas del sector TIC y el CSIRT Nacional para compartir indicadores de nuevas campañas de forma ágil y estandarizada.

- **Auditorías de Terceros y Cadena de Suministro**: Establecer requisitos de ciberseguridad estrictos para proveedores, considerando que el sector es un objetivo clave para ataques de cadena de suministro.

Preparación ante Incidentes

- **Actualización de Playbooks:** Desarrollar guías de respuesta específicas para los TTPs de los actores identificados, especialmente para la contención de comunicaciones de Comando y Control (C2).

- **Simulacros de Crisis (Tabletop):** Realizar ejercicios basados en escenarios de compromiso real de infraestructura crítica para validar la capacidad de toma de decisiones bajo presión.

Acciones Inmediatas (Quick Wins)

- **Bloqueo de Top IOCs:** Ejecutar el bloqueo inmediato de los dominios y direcciones IP asociados a los adversarios con mayor presencia en el reporte, como UNC6395 y APT44.

- **Campaña de Concientización Anti-Phishing:** Alertar al personal administrativo sobre el uso de las 237 URLs de suplantación detectadas, reforzando la verificación de identidades digitales.

- **Revisión de Accesos de Gestión:** Auditar y restringir el acceso a interfaces administrativas expuestas que coincidan con los vectores de ataque (CVE) analizados.

CONCLUSIONES

1. Centralidad de la Infraestructura de Red en el Ataque

- El ecosistema de amenazas está dominado por la **infraestructura de red**, que representa el **72,4%** de la inteligencia recolectada. Con **1.581 dominios (FQDN)** y **1.075 direcciones IP** activas, se concluye que los atacantes priorizan el control de las comunicaciones y la redirección de tráfico sobre el despliegue de archivos. El sector TIC no es solo un blanco, sino que es utilizado como una **plataforma de salto** para interceptar flujos de información nacional.

2. Convergencia y Reutilización de Recursos (Amenaza Multiactor)

- Existe una clara correlación entre grupos de **espionaje estatal (APT)** y **crimen organizado (FIN)**. Se ha detectado que diferentes actores comparten los mismos nodos de salto y servidores de comando y control (C2). Esta "infraestructura como servicio" maliciosa sugiere que el sector TIC colombiano enfrenta un ecosistema interconectado donde una vulnerabilidad explotada por un grupo criminal puede ser rápidamente aprovechada por un actor de espionaje para exfiltración silenciosa.

3. Explotación Persistente de Fallos Conocidos

- La identificación de **198 vulnerabilidades críticas (CVE)** demuestra que los atacantes no dependen exclusivamente de técnicas desconocidas (Zero-days), sino que aprovechan la **ventana de oportunidad** que deja la gestión lenta de parches. Se concluye que el reconocimiento activo (escaneo de puertos y servicios expuestos) es la fase más crítica y constante en el ciclo de ataque actual del país.

4. Sofisticación en la Evasión de Defensas

- El uso de **574 artefactos maliciosos únicos (hashes)**, muchos de ellos polimórficos, indica una alta capacidad de los adversarios para evadir sistemas de detección tradicionales basados en firmas. Los grupos más activos, como **APT44, APT41 y UNC6395**, emplean técnicas de ofuscación y protocolos mimetizados (HTTP/S y DNS) para que el tráfico malicioso parezca actividad legítima de red, dificultando su detección en el monitoreo estándar.

5. Riesgo Crítico para la Cadena de Suministro Digital

- Dado que el sector TIC es el habilitador de servicios para otros sectores (Energía, Salud, Gobierno), se concluye que el objetivo estratégico de los adversarios es el **compromiso de la cadena de suministro**. Un ataque exitoso a un proveedor de servicios de nube o centro de datos en Colombia tiene un efecto dominó que compromete la soberanía tecnológica y la disponibilidad de servicios esenciales para toda la población.

6. Necesidad de una Defensa Proactiva y Colaborativa

- El volumen de **2.803 ataques semanales por organización** reportado evidencia que las defensas reactivas son insuficientes. La conclusión operativa es que se requiere una transición hacia el **Threat Hunting (Caza de Amenazas)** y el intercambio de inteligencia en tiempo real entre empresas del sector y organismos nacionales para bloquear la infraestructura adversaria antes de que ocurra el impacto operativo o la exfiltración de datos.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **Amenaza Avanzada Persistente (APT):** Grupos de atacantes altamente capacitados y con recursos, generalmente respaldados por estados, que ejecutan campañas de intrusión prolongadas y dirigidas.
- **Indicadores de Compromiso (IoC):** Evidencias digitales (como hashes, IPs o dominios) que indican con un alto nivel de confianza que un sistema o red ha sido vulnerado.
- **Tácticas, Técnicas y Procedimientos (TTPs):** Patrones de comportamiento y métodos operativos que describen cómo un actor de amenaza planifica y ejecuta un ataque.
- **Mapeo a MITRE ATT&CK:** Proceso de clasificar las acciones de un atacante dentro de una matriz estandarizada globalmente para comprender sus objetivos y fases.
- **Ciberinteligencia de Amenazas (CTI):** Recolección, análisis y difusión de información sobre amenazas actuales y potenciales para ayudar en la toma de decisiones defensivas.
- **Ciclo de Vida del Ataque:** Las etapas secuenciales que sigue un adversario, desde el reconocimiento inicial hasta la exfiltración de datos o el impacto final.

Infraestructura y Redes

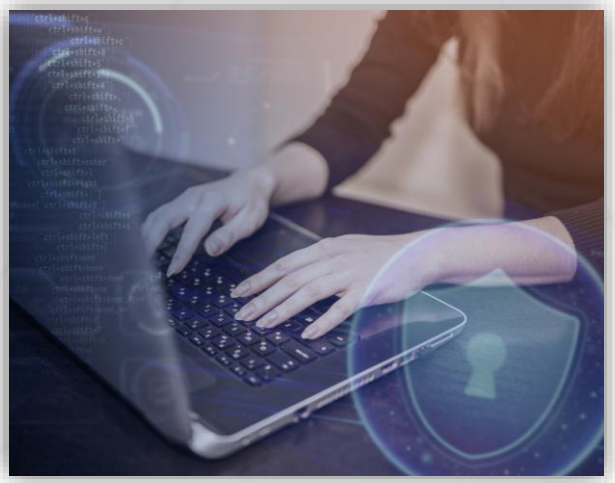
- **Comando y Control (C2):** Infraestructura de servidores utilizada por los atacantes para enviar instrucciones a sistemas comprometidos y recibir datos exfiltrados.
- **FQDN (Fully Qualified Domain Name):** Nombre de dominio completo que especifica la ubicación exacta de un host en la jerarquía del DNS, utilizado frecuentemente para identificar nodos maliciosos.
- **Nodos de Salto (Hop Points):** Servidores intermedios comprometidos que los atacantes utilizan para enmascarar su ubicación real y saltar hacia el objetivo final.
- **Telemetría de Red:** Datos recolectados sobre el tráfico, protocolos y conexiones que permiten visualizar el comportamiento de la infraestructura en tiempo real.
- **Exposición de Superficie:** La suma de todos los puntos vulnerables y servicios accesibles desde internet que un atacante puede intentar explotar.

Herramientas y Malware

- **Hash (SHA-256/MD5):** Firma digital única de un archivo que permite identificar malware de manera inequívoca, incluso si se le cambia el nombre.
- **Artefacto Malicioso:** Cualquier archivo, script o pieza de código creada con el fin de realizar acciones no autorizadas en un sistema.
- **Malware Polimórfico:** Código malicioso diseñado para cambiar su apariencia (firma o estructura) en cada infección para evadir la detección basada en firmas tradicionales.
- **CVE (Common Vulnerabilities and Exposures):** Identificador estándar para una vulnerabilidad de seguridad conocida en software o hardware.
- **Frameworks de Explotación:** Conjuntos de herramientas (como Cobalt Strike o Metasploit) utilizados por analistas y atacantes para automatizar la intrusión en redes.

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