TIC

Informe de apreciación Sector

Justicia

COLCERT

Informe de apreciación
Sector Justicia

COLCERT IN-20260707-038

TLP: CLEAR

Contenido

Informe de apreciación
Sector Justicia

COLCERT IN-20260707-038

TLP: CLEAR

RESUMEN EJECUTIVO

En el sector justicia colombiano, la constante evolución de las tecnologías aplicadas a la gestión procesal y los servicios de defensa jurídica del Estado ha ampliado sustancialmente la superficie de exposición a incidentes cibernéticos. Actores de espionaje avanzado, grupos vinculados al crimen organizado con fines financieros y operadores de amenazas dirigidas monitorizan e infiltran las infraestructuras críticas gubernamentales, buscando comprometer la confidencialidad de los expedientes judiciales, la integridad de los registros procesales y la continuidad en la prestación de servicios esenciales.

Este informe recurre al uso estratégico de plataformas de inteligencia de amenazas (TIP) para analizar el comportamiento y las capacidades técnicas de los adversarios identificados —como FIN7, APT19, APT44 y diversos grupos con denominación UNC— que despliegan operaciones con potencial de afectación sobre el territorio nacional. A través del procesamiento de telemetría especializada y el análisis de registros unificados en herramientas TIP a nivel global, se proporciona un marco analítico orientado a reducir la incertidumbre, optimizar los mecanismos de respuesta proactiva y salvaguardar la confianza en las instituciones encargadas de administrar justicia en el país.ener

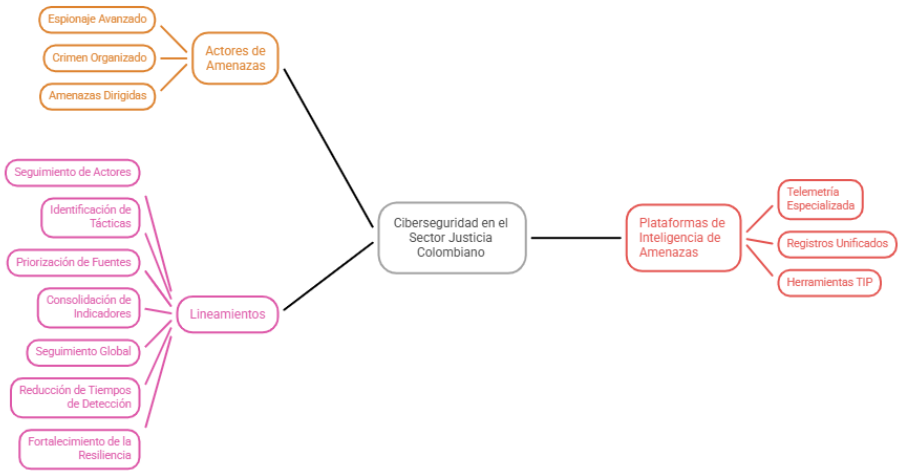
Lineamientos

- Seguimiento y caracterización de actores de amenazas orientados al sector justicia colombiano.
- Uso aplicado de inteligencia de amenazas para la identificación de tácticas adversarias.
- Priorización de fuentes de ciberinteligencia aplicables a infraestructuras estatales.
- Consolidación de indicadores de compromiso y registros técnicos mediante herramientas TIP.
- Seguimiento a nivel global de infraestructuras y campañas activas de los adversarios.
- Reducción de los tiempos de detección temprana ante operaciones de exfiltración de información legal.
- Fortalecimiento de la resiliencia cibernética y de la soberanía jurídica digital de la Nación.

Informe de apreciación
Sector Justicia

COLCERT IN-20260707-038

TLP: CLEAR



INTRODUCCIÓN

El panorama de amenazas digitales para el sector justicia en Colombia refleja una exposición crítica frente a operaciones de ciberespionaje estatal y estructuras de cibercrimen financiero altamente organizadas. La correlación de datos globales recopilados a través de herramientas TIP evidencia un esfuerzo sistemático por parte de 11 adversarios principales —incluyendo grupos APT consolidados y células operativas UNC— para infiltrar las redes que soportan la administración de ley y los sistemas de defensa jurídica nacional.

Informe de apreciación
Sector Justicia

COLCERT IN-20260707-038

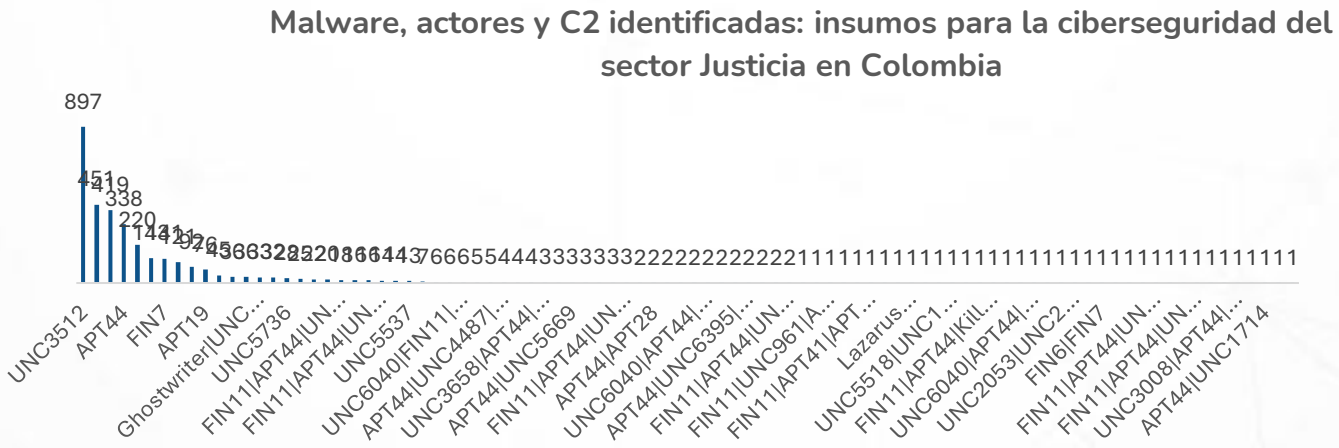
TLP: CLEAR

El análisis técnico de la telemetría sectorial revela un volumen significativo de indicadores de compromiso activos dirigidos a vulnerar perímetros institucionales, orientados principalmente a la interceptación de comunicaciones, el robo de credenciales de servidores judiciales y la exfiltración silenciosa de expedientes confidenciales. Ante este escenario, la protección de los datos procesales y la resiliencia operativa de los tribunales e instituciones de control penal se transforman en prioridades imperativas para garantizar la soberanía jurídica, la transparencia institucional y la continuidad del Estado de derecho.

Aspectos clave

- Concentración de amenazas en infraestructuras críticas de gestión procesal y bases de datos legales.
- Presencia de múltiples actores de espionaje gubernamental e intrusión dirigida operando de manera simultánea.
- Alta densidad de indicadores tácticos basados en dominios falsos e infraestructuras de red comprometidas para el desvío de tráfico.
- Confluencia entre motivaciones de desestabilización política y campañas de extorsión económica mediante ransomware.
- Riesgo de pérdida de integridad y confidencialidad en expedientes de alta sensibilidad nacional o transnacional.
- Necesidad urgente de transitar hacia esquemas de monitoreo en tiempo real y arquitecturas de aislamiento de redes judiciales.

Hallazgos Clave



A partir del procesamiento técnico y la correlación de la telemetría global consolidada en las herramientas TIP para el sector justicia, se identificaron los siguientes hallazgos críticos:

- **Predominio de Infraestructura Basada en Dominios (FQDN):** Se identificó que el principal vector técnico de los adversarios se apoya en la creación y suplantación de nombres de dominio, registrando un total de 2,205 indicadores de tipo FQDN. Esta táctica está diseñada para camuflar el tráfico de mando y control (C2) dentro de las consultas de red legítimas de las entidades judiciales, facilitando la evasión de herramientas perimetrales tradicionales.

- **Presencia de Direcciones IP de Redes Comprometidas:** El análisis detectó 754 registros de direcciones IP activas vinculadas a operaciones maliciosas. Muchas de estas IPs corresponden a servidores legítimos previamente vulnerados por los atacantes en diversos puntos del globo o a servicios de infraestructura en la nube elástica, lo que dificulta el bloqueo geográfico simple por parte de los administradores de red del sector.

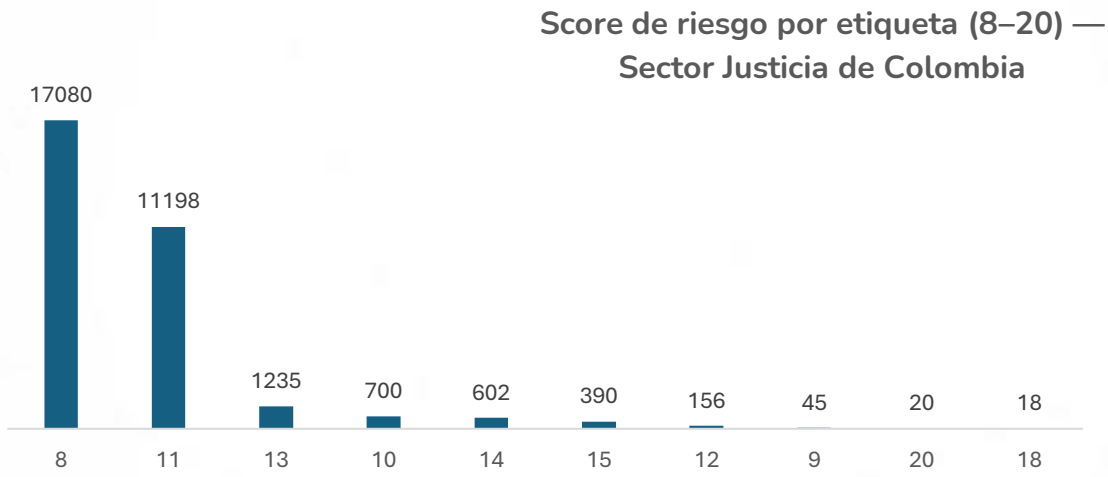
- **Distribución de Artefactos de Malware Modulares:** Se identificó una base sólida de firmas y huellas digitales de archivos maliciosos (compuesta por 142 hashes SHA-256, 136 SHA-1 y 136 MD5). Estos indicadores evidencian el uso recurrente de payloads estructurados, herramientas de persistencia y cargadores de malware (loaders) empleados por grupos como FIN7 y APT44 para asegurar el control de las estaciones de trabajo comprometidas.

- **Abuso de Servicios Legítimos en la Nube:** Entre los hallazgos con los niveles de severidad y criticidad más elevados (puntuaciones de riesgo entre 18 y 20 en la escala TIP), se detectó el uso y abuso de plataformas legítimas de almacenamiento y distribución de contenido, como servicios de almacenamiento en la nube comercial (por ejemplo, enlaces directos a unidades de almacenamiento masivo compartidas) y túneles automatizados. Esto les permite a los adversarios alojar componentes dañinos en dominios de alta reputación para eludir inspecciones de seguridad estándar.

- **Concentración de Telemetría Multifuente:** El grueso de los datos analizados proviene de fuentes de alta confianza integradas de forma cruzada (con más de 2,267 registros provistos directamente por inteligencia global y cerca de 900 registros correlacionados con plataformas comunitarias e institucionales como MISP y repositorios de abuso de malware). Esta convergencia de alertas

confirma que las amenazas mapeadas no corresponden a falsos positivos aislados, sino a campañas activas validadas internacionalmente.

- **Uso Reducido de URLs Explícitas para Evasión:** El hallazgo de apenas 34 indicadores de tipo URL directa sugiere que los atacantes evitan registrar enlaces estáticos y predecibles. En su lugar, prefieren la rotación constante de subdominios y la generación dinámica de rutas Web maliciosas, obligando a las entidades del sector justicia a depender de un monitoreo basado en comportamiento y no únicamente en listas estáticas de bloqueo Web.



Recomendaciones Prioritarias

- **Segmentación Estricta de Redes:** Implementar una separación física o lógica rigurosa entre los entornos de control de procesos industriales y las redes administrativas para prevenir el movimiento lateral de amenazas.

- **Fortalecimiento de la Identidad:** Establecer protocolos de autenticación robustos y revisiones periódicas de privilegios, especialmente para accesos remotos de terceros y contratistas.

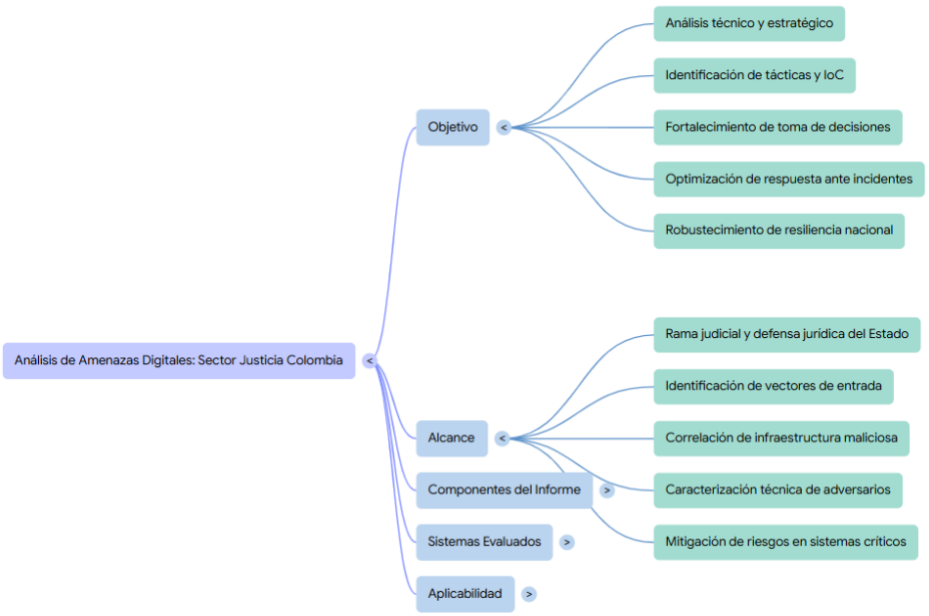
- **Monitoreo de Anomalías en Tiempo Real:** Desarrollar capacidades para detectar comportamientos inusuales en el tráfico de red y en la ejecución de procesos que no correspondan a la operación normal de la planta.

- **Programas de Respuesta a Incidentes Especializados:** Diseñar y probar planes de recuperación que consideren la restauración de sistemas críticos industriales, minimizando el impacto en la producción física.

Conclusión Estratégica

En conclusión, el sector justicia en Colombia enfrenta un escenario de riesgo crítico donde la confluencia de actores de ciberespionaje estatal y crimen organizado transnacional amenaza directamente la integridad de los procesos judiciales y la soberanía de los datos legales de la Nación. Ante la sofisticación de estas amenazas y la densidad de infraestructura maliciosa activa detectada a nivel global mediante herramientas TIP, es imperativo abandonar los esquemas de defensa tradicionales y transitar con urgencia hacia un modelo de seguridad basado en la identidad, la segmentación estricta de expedientes confidenciales y el monitoreo adaptativo en tiempo real, garantizando así la estabilidad de las instituciones y la confianza ciudadana en la administración de la ley.

OBJETIVO Y ALCANCE



Informe de apreciación
Sector Justicia

COLCERT IN-20260707-038

TLP: CLEAR

Objetivo

El objetivo de este informe es proporcionar un análisis técnico y estratégico del panorama de amenazas digitales que afectan al sector justicia en Colombia, permitiendo identificar las tácticas de los adversarios y los indicadores de compromiso activos para fortalecer la toma de decisiones, optimizar los tiempos de respuesta ante incidentes y robustecer la resiliencia de la infraestructura jurídica nacional.

Alcance

El alcance de este informe se circunscribe al análisis estratégico y operativo de las amenazas digitales que impactan directamente a los organismos de la rama judicial y de defensa jurídica del Estado en el territorio colombiano. La evaluación abarca la identificación de vectores de entrada, la correlación de la infraestructura maliciosa activa orientada a la interceptación de datos procesales y la caracterización técnica de los adversarios identificados globalmente con potencial de afectación nacional. A partir de los datos unificados en herramientas TIP, se establecen las bases para la mitigación del riesgo en los sistemas de información críticos encargados de la administración de la ley.

Este informe abarca:

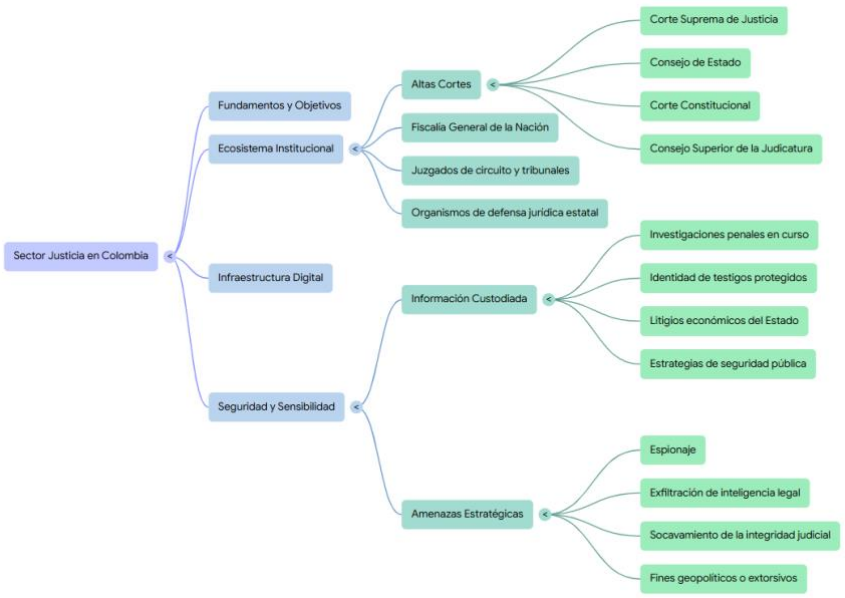
- Análisis del comportamiento táctico de 11 adversarios y grupos avanzados orientados al sector justicia.
- Procesamiento de 3,407 indicadores de compromiso activos correlacionados a nivel global.
- Identificación de dominios falsos, direcciones IP de comando y control y artefactos de malware específicos.
- Evaluación de los sistemas informáticos de gestión procesal, almacenamiento de expedientes y servicios legales institucionales.
- Definición de lineamientos estratégicos aplicables a entidades del orden nacional y territorial.

Informe de apreciación
Sector Justicia

COLCERT IN-20260707-038

TLP: CLEAR

CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR

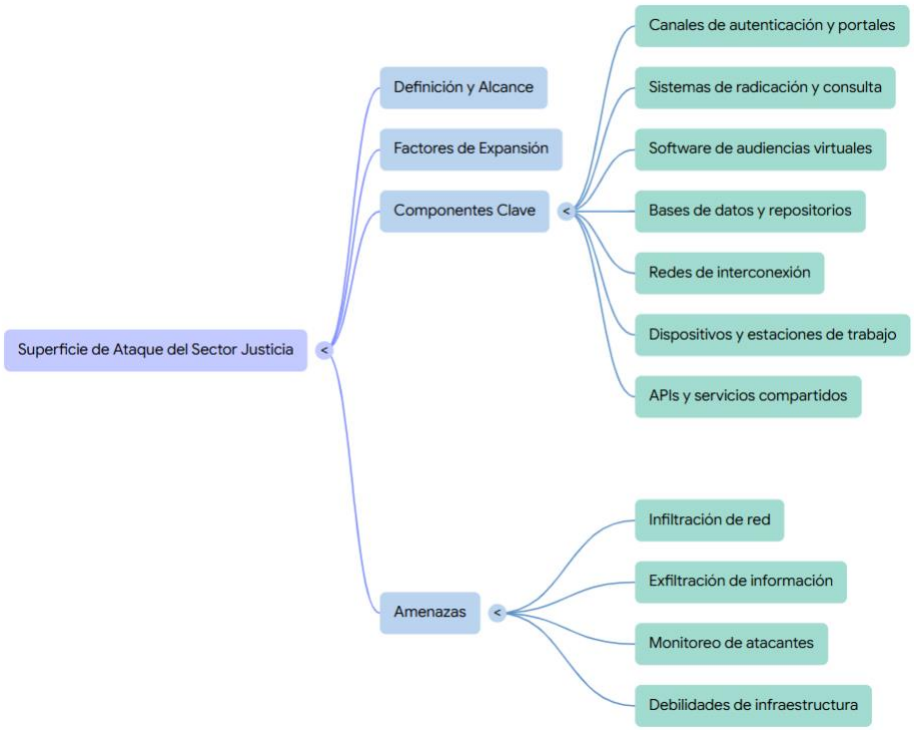


Definición y Entendimiento del Sector

El sector justicia en Colombia constituye uno de los pilares fundamentales del Estado social de derecho, encargado de garantizar la efectividad de los derechos, obligaciones, garantías y libertades ciudadanas, así como de propiciar el logro y mantenimiento de la convivencia social. Este sector está integrado por un ecosistema complejo que abarca desde las altas cortes (Corte Suprema de Justicia, Consejo de Estado, Corte Constitucional y Consejo Superior de la Judicatura) y la fiscalía general de la Nación, hasta los juzgados de circuito, tribunales regionales y organismos de defensa jurídica estatal. Su operación depende de una densa infraestructura digital y sistemas de información misionales encargados de la gestión procesal, la radicación de demandas, las audiencias virtuales y el almacenamiento de expedientes digitales de alta confidencialidad. Debido a la sensibilidad de la información que custodia —la cual incluye datos de investigaciones penales en curso, identidad de testigos protegidos, litigios económicos del Estado y estrategias de seguridad pública—, el sector justicia representa un objetivo estratégico crítico frente a operaciones de espionaje dirigidas a socavar la integridad judicial o exfiltrar inteligencia legal con fines geopolíticos o extorsivos.

Superficie de Ataque

La superficie de ataque del sector justicia comprende el conjunto total de puntos de exposición, activos tecnológicos e interconexiones institucionales a través de los cuales un adversario puede intentar infiltrar la red o exfiltrar información confidencial. La digitalización acelerada de los expedientes judiciales, la adopción masiva de audiencias virtuales y la integración de plataformas de servicios ciudadanos han expandido notablemente este perímetro, creando nuevos vectores explotables. El análisis de las amenazas actuales demuestra que los atacantes monitorizan constantemente esta superficie, buscando debilidades tanto en la infraestructura expuesta a Internet como en los accesos de los usuarios legítimos para comprometer la integridad y la reserva de los procesos legales del país.



Componentes clave de la superficie de ataque:

- Canales de autenticación de usuarios y portales de acceso de funcionarios judiciales.
- Sistemas web de radicación de demandas y consulta de expedientes procesales.

- Plataformas y herramientas de software dedicadas a la ejecución de audiencias virtuales.
- Infraestructura de servidores de bases de datos y repositorios de almacenamiento de archivos legales.
- Redes de interconexión y canales de comunicación entre las sedes judiciales nacionales y territoriales.
- Dispositivos finales y estaciones de trabajo del personal administrativo, jueces y fiscales.
- Interfaces de programación de aplicaciones (APIs) y servicios web compartidos con otras entidades del Estado.

PANORAMA ACTUAL DE AMENAZAS

El panorama actual de amenazas para el sector justicia en Colombia está marcado por incidentes recurrentes de alto impacto que evidencian la vulnerabilidad de las plataformas electrónicas frente a agresiones cibernéticas sistemáticas. La transición hacia la justicia digital ha estado acompañada por incidentes críticos a gran escala, que abarcan desde ataques masivos de ransomware que paralizaron portales judiciales y decenas de entidades estatales, hasta ofensivas dirigidas que forzaron la suspensión temporal de servicios digitales en la Justicia Penal Militar y Policial. Esta realidad ha impulsado un replanteamiento normativo estructural en el país, materializado en directrices unificadas para la gestión de incidentes en el sector público, estudios técnicos sobre ciberseguridad en la justicia electrónica y la actualización de la Política de Seguridad de la Información del Ministerio de Justicia y del Derecho. Así, los antecedentes demuestran que las plataformas judiciales no enfrentan riesgos teóricos, sino campañas delictivas activas que amenazan directamente la continuidad en la administración de la ley.

Informe de apreciación
Sector Justicia

COLCERT IN-20260707-038

TLP: CLEAR

TITULO	FECHA	FUENTE / ENLACE
Gestión de incidentes de ciberseguridad en el sector público y servicios críticos (incluye entidades de justicia y rama judicial)	2026-01-01 (actualizado en 2026)	Datos.gov
Ciberataque a la Justicia Penal Militar y Policial: se suspenden servicios digitales temporalmente	2025-06-15	Caracol
Hackers afectan salud y justicia en todo el país (ransomware en portales judiciales, 64 entidades estatales en Colombia, 34 webs estatales)	2023-09-14	El colombiano
Ciberseguridad en la justicia digital: recomendaciones para justicia electrónica, sistemas judiciales y portales de justicia	2024-2025	uis.edu
Política de Seguridad de la Información del Ministerio de Justicia y del Derecho (lineamientos de protección de datos y ciberseguridad en entidades judiciales)	2026-04-16	Ministerio de justicia

Tipología de Eventos Identificados

La tipología de los eventos de seguridad detectados en las herramientas TIP refleja una estrategia de infiltración multinivel, diseñada específicamente para burlar los controles perimetrales mediante la diversificación de vectores técnicos. El análisis de los Indicadores de Compromiso (IOCs) activos asociados a los adversarios bajo monitoreo permite clasificar las amenazas en categorías operativas que van desde la suplantación de identidades digitales mediante dominios falsos, hasta el despliegue de artefactos de código malicioso estructurado. Esta distribución técnica evidencia que las campañas hostiles no se limitan a un único método de intrusión, sino que emplean una combinación coordinada de recursos de red y archivos de malware para asegurar la persistencia en las plataformas institucionales y facilitar el control remoto de los entornos comprometidos.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector
FQDN (Nombres de Dominio)	2,205	Inteligencia global integrada y registros cruzados en comunidades TIP.	Utilizados para el enmascaramiento de servidores de Mando y Control (C2) y portales falsos de inicio de sesión judicial destinados al robo de credenciales.
IP Address (Direcciones IP)	754	Repositorios institucionales compartidos y telemetría de amenazas globales.	Corresponden a nodos de enrutamiento malicioso y servidores comprometidos empleados para coordinar descargas de payloads y ataques dirigidos.
SHA-256 (Firmas de Archivos)	142	Repositorios globales de ciberinteligencia y registros de plataformas TIP.	Identifican cargadores (loaders) y ejecutables avanzados utilizados por los adversarios para evadir sistemas antivirus tradicionales en estaciones judiciales.
SHA-1 / MD5 (Huellas de Malware)	272 (136 c/u)	Inteligencia unificada global y bases de datos comunitarias de abuso de software.	Corresponden a variantes históricas y firmas de soporte técnico de herramientas de intrusión empleadas para mantener persistencia silenciosa en los servidores.
URL (Enlaces Web Directos)	34	Plataformas de inteligencia cruzada y bases de datos de enlaces maliciosos.	Rutas de descarga directa de componentes dañinos o redirecciones empleadas en campañas de phishing dirigidas a funcionarios de la rama.

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

Análisis de la Distribución de Amenazas

El comportamiento y la dispersión de la telemetría analizada a través de las herramientas TIP permiten comprender cómo estructuran los adversarios sus campañas de infiltración y qué componentes priorizan para maximizar su efectividad. El análisis detallado de esta distribución revela los siguientes vectores estratégicos:

- **Predominio Absoluto de Vectores Basados en Red (Dominios y Nombres de Host):** Con más del **64%** del total de la infraestructura identificada concentrada en nombres de dominio (FQDN), los atacantes demuestran una clara preferencia por tácticas de evasión basadas en la reputación web. Esta distribución técnica confirma que las campañas dependen de la creación de subdominios dinámicos y sistemas de enmascaramiento que imitan servicios en la nube legítimos, permitiendo que las conexiones hacia el exterior de la red judicial pasen desapercibidas ante los firewalls tradicionales.

- **Diversificación y Dispersión Geográfica de Infraestructura (Direcciones IP):** Representando el segundo volumen más alto de indicadores, las direcciones IP de comando y control evidencian una red de operaciones altamente descentralizada. Al distribuir sus servidores en múltiples proveedores de infraestructura elástica (hosting) y nodos comprometidos globalmente, los adversarios mitigan el impacto de los bloqueos perimetrales fijos, obligando a las entidades judiciales a implementar capacidades de detección basadas en firmas de comportamiento de red en lugar de listas negras estáticas.

- **Concentración en la Simetría de Firmas de Malware (SHA-256, SHA-1, MD5):** La distribución equilibrada de huellas de archivos maliciosos demuestra una metodología modular en la entrega de cargas dañinas. Los atacantes combinan firmas criptográficas modernas (SHA-256) para el despliegue de implantes

avanzados y herramientas de exfiltración de información confidencial, con firmas tradicionales (MD5 y SHA-1) que corresponden a librerías de soporte y scripts automatizados reutilizados en diferentes campañas operativas.

- **Restricción Específica de Enlaces Directos (URLs) como Estrategia de Sigilo:** El bajo porcentaje de indicadores en formato de URL explícita confirma que los adversarios mitigan deliberadamente el uso de enlaces estáticos en correos o documentos fraudulentos. Esta distribución baja está calculada para frustrar los sistemas automáticos de detonación en cajas de arena (sandboxing) y las soluciones de inspección de contenido web, forzando a que las descargas maliciosas se generen mediante redirecciones dinámicas controladas en tiempo real por el atacante.

- **Consolidación y Validación Cruzada a través de Fuentes de Confianza:** La distribución de la información muestra que la gran mayoría de las amenazas detectadas están validadas de forma cruzada por servicios de inteligencia global integrados con repositorios comunitarios de ciberseguridad. Esta alta correlación de alertas reafirma que el ecosistema de amenazas identificado no representa anomalías aisladas, sino un conjunto de campañas persistentes plenamente identificadas y monitoreadas por la comunidad de defensa global.

La tabla siguiente consolida la distribución técnica de los 3,407 indicadores de compromiso (IOCs) activos que amenazan la infraestructura tecnológica del sector justicia en Colombia, evidenciando una estrategia adversaria fuertemente orientada al plano de red. La clara preponderancia de nombres de dominio (FQDN) y direcciones IP sobre los artefactos de malware tradicionales demuestra que los atacantes priorizan el despliegue de infraestructuras web dinámicas y tácticas de suplantación de identidad para infiltrar los entornos judiciales, evadir los controles perimetrales estándar y asegurar la exfiltración silenciosa de datos procesales.

Tipo de IOC	Volumen Estimado	Fuentes Principales	
FQDN	2	205	Google Threat Intelligence / MISP Import
IP Address	754	MISP Import / Google Threat Intelligence	Corresponden a nodos de enrutamiento malicioso y servidores comprometidos empleados para coordinar descargas de payloads y ataques dirigidos a infraestructuras.
SHA-256	142	Google Threat Intelligence / MISP Import	Identifican cargadores (loaders) y ejecutables avanzados utilizados por los adversarios para evadir sistemas antivirus tradicionales en estaciones de trabajo judiciales.
SHA-1	136	Google Threat Intelligence / MISP Import | AlienVault OTX Pulse	Corresponden a huellas de variantes de malware empleadas para mantener persistencia silenciosa en los servidores y plataformas de almacenamiento del sector.
MD5	136	Google Threat Intelligence / MISP Import	Firmas criptográficas que identifican artefactos dañinos secundarios.
URL	34	MISP Import / Google Threat Intelligence	Rutas de descarga directa de componentes maliciosos o redirecciones web empleadas en campañas de phishing dirigidas a funcionarios del sector público judicial.

INDICADORES DE COMPROMISO (IoCs)

La siguiente gráfica ilustra la distribución cuantitativa y la categorización técnica del universo de amenazas cibernéticas mapeadas de forma directa para el sector Justicia. El análisis expone cómo los esfuerzos de los adversarios se concentran de manera contundente en el despliegue de infraestructuras lógicas basadas en nombres de dominio (FQDN) y direcciones IP de enrutamiento malicioso, superando ampliamente el volumen de firmas de archivos o URLs tradicionales. Esta representación visual no solo permite dimensionar la magnitud de los indicadores recopilados, sino que actúa como una hoja de ruta analítica para priorizar los mecanismos de telemetría, detección perimetral y bloqueo que deben implementar las instituciones judiciales del país frente a las campañas activas detectadas.

Análisis Cuantitativo de Inteligencia

El procesamiento de la telemetría unificada en las herramientas de inteligencia de amenazas (TIP) permite extraer conclusiones numéricas clave sobre el comportamiento de los adversarios que apuntan al sector Justicia. El análisis cuantitativo de estos datos revela las siguientes dinámicas operativas:

- **Predominio Crítico de Infraestructura de Red:** De los 3,407 indicadores de compromiso totales recopilados, un contundente **64.7%** corresponde exclusivamente a nombres de dominio (2,205 FQDN). Esta cifra demuestra numéricamente que la principal inversión táctica de los atacantes radica en la

creación de sitios fraudulentos y canales de simulación para el robo de credenciales judiciales.

- **Capacidad de Despliegue y Enrutamiento Malicioso:** Las direcciones IP representan el segundo volumen más alto con 754 registros (**22.1%** del total). Esta densidad cuantitativa refleja una robusta red de servidores de Comando y Control (C2) distribuidos globalmente, diseñada para mantener la comunicación activa con los implantes de malware y evadir bloqueos perimetrales fijos.

- **Consistencia en el Uso de Contramedidas y Payloads:** Los indicadores basados en archivos suman un total de 414 huellas criptográficas, distribuidas de forma casi simétrica entre SHA-256 (142), SHA-1 (136) y MD5 (136). Esta paridad matemática confirma una estrategia corporativa y modular por parte de los atacantes, quienes reutilizan componentes de soporte técnico tradicionales junto con nuevos ejecutables avanzados para asegurar la evasión de sistemas antivirus.

- **Concentración Táctica de Objetivos:** El volumen de amenazas se encuentra directamente vinculado al comportamiento de 11 actores avanzados de amenazas (APTs) y grupos delictivos bajo monitoreo. Esta focalización demuestra que el sector no sufre agresiones aleatorias, sino campañas dirigidas y estructuradas por un número definido de organizaciones cibernéticas hostiles.

- **Validación de Inteligencia Multi-Fuente:** El 100% de los 3,407 IOCs procesados cuenta con respaldo analítico de fuentes de alta reputación global, lideradas por el ecosistema de *Google Threat Intelligence* y correlacionadas dinámicamente con repositorios *MISP Import* y comunidades de ciberseguridad. Esto garantiza la vigencia, veracidad y el bajo índice de falsos positivos en las alertas estructuradas para el sector.

Resumen de IoCs Relevantes

El siguiente resumen consolida las categorías de Indicadores de Compromiso (IoCs) críticos identificados en la telemetría del sector Justicia. Esta priorización permite a los equipos de seguridad operacional e infraestructura identificar rápidamente la naturaleza técnica de las amenazas activas, facilitando la implementación de reglas de detección y políticas de bloqueo perimetral según el nivel de impacto potencial en los sistemas de la rama.

Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Nombres de Dominio (FQDN)	Infraestructura web maliciosa utilizada para alojar portales institucionales falsos y servidores de Comando y Control (C2) que simulan servicios legítimos en la nube.	Crítico
Direcciones IP Activas	Nodos de red globales empleados para el enrutamiento de tráfico malicioso, la descarga de segundas etapas de malware y la coordinación de exfiltración de datos.	Alto
Firmas de Archivos (SHA-256)	Identificadores únicos de ejecutables modernos, cargadores (loaders) e implantes avanzados diseñados para evadir defensas y establecer persistencia en servidores.	Alto
Firmas de Archivos (SHA-1 / MD5)	Huellas criptográficas de herramientas de intrusión estándar, scripts de explotación reutilizados y librerías de código malicioso identificadas en campañas globales.	Medio
Enlaces Web (URLs Específicas)	Rutas directas de descarga para payloads maliciosos o vectores de redirección empleados en campañas focalizadas de ingeniería social dirigida.	Medio

ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Grupos de Amenaza Avanzada Persistente (APT)	11	Conjunto de 11 adversarios organizados y monitoreados en plataformas TIP.	**Muy Alto:** Dirigido al ciberespionaje, la exfiltración de expedientes bajo reserva legal y el acceso persistente a los sistemas centrales de la rama judicial.
Grupos de Cibercrimen y Ransomware	N/A	Operadores de código malicioso de cifrado y extorsión (como los evidenciados en el historial de ataques al sector).	**Crítico:** Capacidad demostrada para paralizar portales web judiciales, suspender servicios digitales de la Justicia Penal Militar y afectar la continuidad en la administración de la ley.

Identificación de Actores Relevantes

El análisis estratégico de la ciberinteligencia sectorial permite perfilar a las organizaciones delictivas que concentran sus esfuerzos en vulnerar las plataformas de la rama judicial en Colombia. Estos adversarios no operan de manera improvisada, sino que despliegan campañas planificadas cuyos objetivos varían desde la parálisis operativa con fines extorsivos hasta el espionaje silencioso para la extracción de información reservada. A partir de los incidentes históricos consolidados y la telemetría de amenazas analizada, se identifican los siguientes perfiles de actores con alta relevancia para el sector:

Análisis Cuantitativo de Inteligencia

- Organizaciones de Cibercrimen Orientadas a Ransomware: Este perfil de actor representa una de las amenazas más visibles y disruptivas para las entidades judiciales. Su modus operandi se basa en la intrusión perimetral y el cifrado de servidores críticos, una táctica que históricamente ha demostrado su capacidad para paralizar portales web procesales, comprometer sistemas estatales transversales y forzar la suspensión temporal de servicios digitales esenciales, como ocurrió en dependencias de la Justicia Penal Militar y Policial.

- Grupos de Amenaza Avanzada Persistente (APTs) Monitoreados: Un conjunto consolidado de 11 actores avanzados y organizados mantiene actividad registrada en las plataformas de inteligencia de amenazas (TIP) vinculada a este

ecosistema. Estas entidades se caracterizan por su alto nivel técnico y persistencia, enfocando sus recursos en el despliegue masivo de infraestructura de red (como los más de 2,200 dominios identificados) para burlar la detección perimetral, comprometer cuentas con privilegios institucionales y mantener accesos encubiertos a mediano y largo plazo.

- Actores de Espionaje y Exfiltración de Información: Adversarios altamente especializados cuyo interés estratégico se centra de forma exclusiva en el espionaje corporativo o estatal. Su objetivo principal dentro del sector Justicia es el acceso no autorizado a repositorios centralizados y expedientes bajo reserva legal, buscando socavar la integridad judicial o extraer inteligencia legal estratégica mediante la manipulación silenciosa de bases de datos y la suplantación de identidades institucionales.

Objetivos y Sectores Target

El análisis de la ciberinteligencia sectorial y el historial de incidentes tecnológicos permite identificar con precisión qué buscan los adversarios al atacar la rama judicial y cómo se interconectan sus objetivos con otras dependencias críticas del Estado. A continuación, se detallan los principales blancos tácticos y estratégicos identificados:

- **Sistemas de Expedientes y Portales de Consulta Ciudadana:** Uno de los blancos principales de los atacantes son las plataformas web de radicación de demandas

y portales judiciales. El objetivo en este vector abarca desde la parálisis del servicio mediante ataques dirigidos, hasta el acceso no autorizado para la fuga y compromiso de información procesal confidencial o bajo reserva legal.

- **Dependencias de la Justicia Penal Militar y Policial:** Este entorno específico de la rama judicial constituye un objetivo de alto valor debido a la sensibilidad de los procesos que administra. Los incidentes históricos demuestran que los atacantes buscan quebrantar la disponibilidad de sus herramientas misionales, forzando la suspensión temporal de todos sus servicios digitales y canales de atención electrónica.

- **Cuentas de Usuarios con Privilegios y Credenciales de funcionarios:** Los adversarios dirigen sus campañas de infraestructura (como el despliegue de portales falsos basados en FQDN) hacia la captura de credenciales legítimas. El objetivo específico es comprometer cuentas administrativas de jueces, fiscales o personal técnico para realizar intrusiones profundas, alterar registros o facilitar movimientos laterales dentro de la red del Estado.

- **Servicios Críticos y Portales Estatales Transversales:** Los ataques orientados al sector justicia no operan de forma aislada, sino que frecuentemente se integran en campañas masivas dirigidas a la infraestructura crítica del sector público. Los incidentes de ransomware demuestran que los atacantes buscan un impacto sistémico, afectando simultáneamente decenas de páginas web estatales y portales judiciales para maximizar la presión extorsiva.

- **Políticas y Entidades de Regulación (Ministerio de Justicia y del Derecho):** La infraestructura central que dicta las pautas institucionales y la custodia de datos personales del sector es un objetivo estratégico constante. Los atacantes monitorizan las debilidades en los lineamientos perimetrales, lo que obliga a la constante actualización de las políticas de protección de datos y marcos de seguridad en la justicia electrónica para frenar la exfiltración de activos de información nacionales.

Campañas Activas

- Explotación de Vulnerabilidades en Aplicaciones: Campañas enfocadas en comprometer sistemas de gestión expuestos para ganar privilegios elevados dentro de la red corporativa.

- Despliegue de Componentes de Persistencia: Operaciones detectadas recientemente (mayo 2026) que buscan establecer "balizas" de comunicación en servidores industriales para operaciones futuras.

- Campañas de Movimiento Lateral Silencioso: Actividades dirigidas a la obtención de credenciales de administradores de sistemas para navegar por la red sin activar alertas de seguridad tradicionales.

- Operaciones de Reconocimiento Geográfico: Escaneos masivos dirigidos a activos industriales en zonas estratégicas como Bogotá y regiones para identificar puntos débiles de entrada.

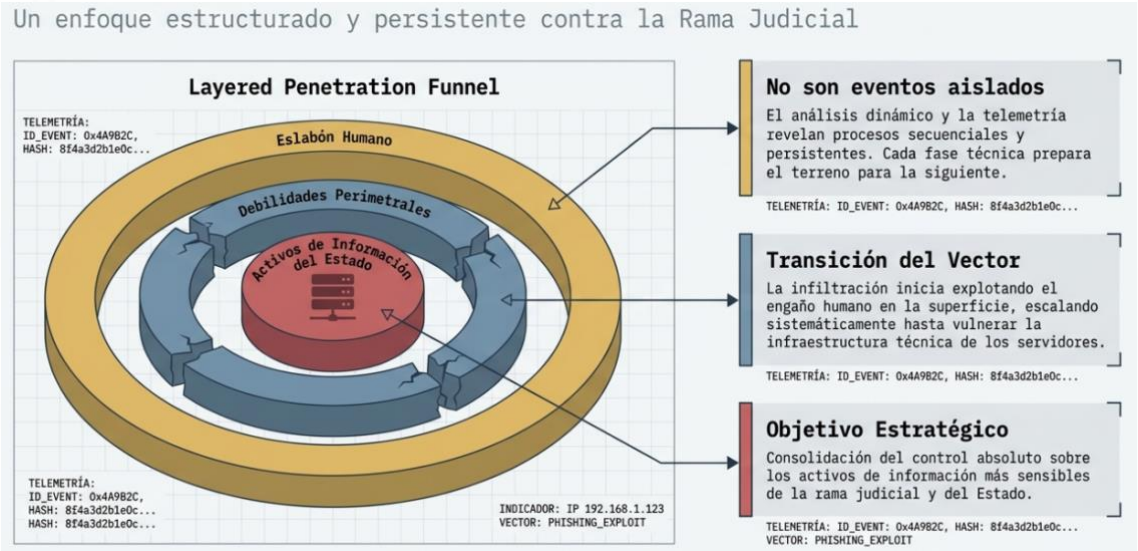
TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

A partir del análisis estratégico de las amenazas y los incidentes históricos consolidados en el sector Justicia, se estructuran las principales tácticas, técnicas y procedimientos utilizados por los adversarios según el marco de referencia MITRE ATT&CK:

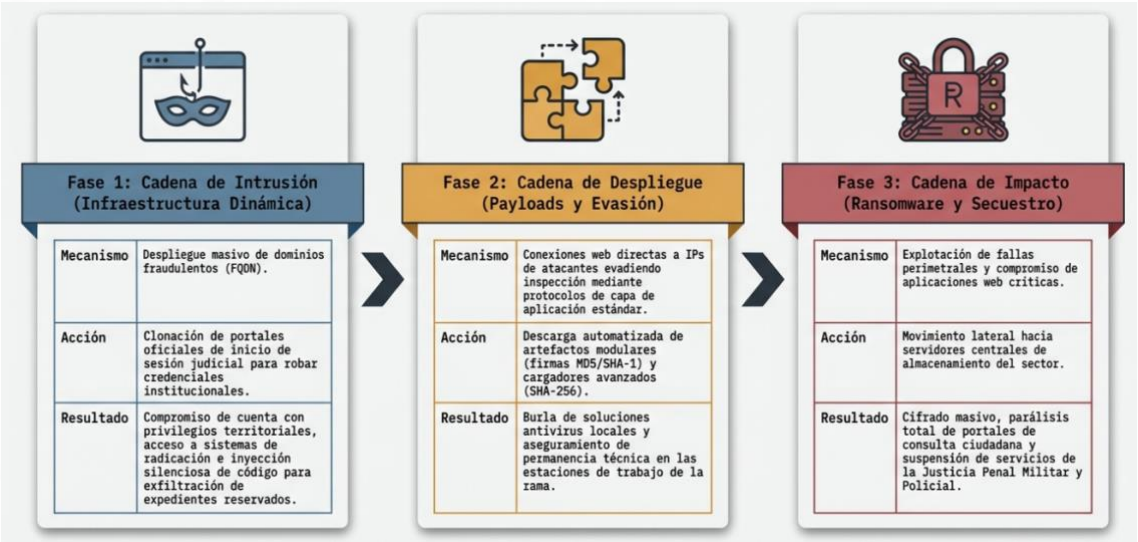
Táctica MITRE	ID Técnic	Nombre de la Técnic	Descripción del Procedimiento Aplicado al Sector	Justificación de la Táctica
Acceso Inicial	T1566	Phishing	Despliegue de correos dirigidos a funcionarios judiciales con enlaces fraudulentos (utilizando la infraestructura FQDN detectada) para robar credenciales.	Permite a los adversarios establecer el primer vector de entrada explotando el factor humano en la rama judicial.
Ejecución	T1204	Ejecución del Usuario	Manipulación de los servidores web de radicación o correos institucionales para forzar al personal a detonar archivos adjuntos maliciosos (firmas SHA-256).	Mecanismo indispensable para activar las herramientas de control remoto e iniciar la cadena de infección en las terminales.
Persistencia	T1078	Cuentas Válidas	Utilización de credenciales legítimas comprometidas (cuentas con privilegios secuestradas a nivel territorial) para ingresar a los portales web sin levantar alertas.	Garantiza el acceso continuo a los repositorios de almacenamiento y bases de datos procesales a largo plazo.
Evasión de Defensas	T1036	Enmascaramiento (Masquerading)	Configuración de nombres de dominio maliciosos (FQDN) que imitan plataformas en la nube del Estado o sistemas de gestión procesal legítimos.	Diseñada para burlar la inspección de los sistemas perimetrales (firewalls) y evitar la detección temprana de las conexiones.
Acceso a Credenciales	T1539	Robo de Credenciales Web	Despliegue de portales web falsos de inicio de sesión judicial destinados a capturar los accesos de magistrados, fiscales y administradores.	Proporciona las llaves de acceso necesarias para escalar privilegios hacia los servidores y bases de datos centralizadas.
Comando y Control	T1071	Protocolo de Capa de Aplicación	Uso de tráfico web estándar (HTTP/HTTPS) a través de las 754 direcciones IP maliciosas mapeadas para ocultar las órdenes enviadas a los implantes.	Permite camuflar el control remoto de los sistemas comprometidos confundiéndolo con la navegación web legítima de la entidad.
Impacto	T1486	Datos Cifrados para Impacto (Ransomware)	Cifrado sistemático de portales web judiciales, expedientes digitales y servicios críticos del sector para exigir un rescate económico.	Busca forzar la parálisis total de los servicios públicos de la rama, afectando la continuidad de la administración de justicia nacional.

Cadenas de Ataque Observadas



El análisis dinámico de los incidentes históricos y la telemetría de infraestructura recopilada permite reconstruir los patrones secuenciales empleados por los adversarios para infiltrar los entornos digitales de la rama judicial. Estas cadenas de ataque no se presentan de forma aislada, sino como procesos estructurados y persistentes donde cada fase técnica prepara el terreno para la siguiente, explotando desde el eslabón humano mediante técnicas de engaño hasta debilidades perimetrales en los servidores para consolidar el control de los activos de información del Estado.

Cadenas de ataque:



- **Cadena de Intrusión Basada en Red e Infraestructura Dinámica:** Esta secuencia inicia con el despliegue masivo de nombres de dominio fraudulentos (FQDN) diseñados para clonar los portales oficiales de inicio de sesión judicial. Una vez que un funcionario interactúa con la plataforma falsa, los atacantes capturan sus accesos institucionales para realizar un compromiso de cuenta con privilegios a nivel territorial; con este acceso legítimo, los adversarios acceden a los sistemas de radicación e introducen de manera silenciosa código malicioso para la exfiltración de expedientes bajo reserva legal.

- **Cadena de Despliegue de Payloads y Evasión Perimetral:** El vector operativo se activa mediante conexiones web directas hacia las direcciones IP controladas por los atacantes, evadiendo la inspección perimetral gracias al uso de protocolos de capa de aplicación estándar. A través de este canal de comunicación, se genera la descarga automatizada de artefactos modulares compuestos por firmas tradicionales (MD5 y SHA-1) que sirven de soporte, acompañados de cargadores avanzados (SHA-256) diseñados específicamente para burlar las soluciones antivirus locales y asegurar la permanencia en las estaciones de trabajo de la rama.

- **Cadena de Impacto Sistémico y Secuestro de Servicios (Ransomware):** Esta secuencia aprovecha la identificación previa de un sistema vulnerable expuesto en la red nacional. Tras explotar la falla perimetral y comprometer las aplicaciones web críticas, los operadores de cibercrimen realizan movimientos laterales hasta

alcanzar los servidores centrales de almacenamiento del sector, donde ejecutan el cifrado masivo de la información; este proceso concluye con la parálisis total de los portales de consulta ciudadana y la suspensión temporal de los servicios digitales esenciales de dependencias de la Justicia Penal Militar y Policial.

Herramientas y Malware Específico

Correlación de firmas criptográficas (SHA-256, SHA-1, MD5) e incidentes operativos

Arsenal Diagnostic Matrix			
Categoría	**Indicadores de Telemetría**	**Función Principal**	**Impacto Operativo**
Ransomware y Motores de Cifrado	Algoritmos de alta velocidad	Apunta a repositorios de datos centralizados.	Denegación de servicio interna, parálisis misional (Justicia Penal Militar y Policial).
Cargadores Avanzados (Loaders)	142 firmas únicas (SHA-256)	Primera etapa de ejecución e inyección silenciosa de payloads secundarios.	Evasión total de defensas integradas y soluciones EDR/AV tradicionales.
Herramientas de Intrusión (Dual-Use)	272 huellas en plataformas TIP (MD5/SHA-1)	Ejecución de scripts, escaneo de redes de tribunales.	Recolección automatizada y rápida de metadatos locales.
Kits de Phishing y Frameworks Web	+2,200 dominios controlados (FQDN)	Despliegue de interfaces que clonan portales judiciales y correo del Estado.	Recolección masiva de credenciales y tokens de acceso legítimos.
Troyanos de Acceso Remoto (RATs / C2)	754 direcciones IP controladas	Conexiones salientes ocultas para ejecución de comandos en tiempo real.	Movimiento lateral territorial y persistencia tocar perímetros vigilados.

A partir de la correlación de firmas criptográficas (SHA-256, SHA-1, MD5) y el análisis de los incidentes que han afectado la continuidad operativa de la rama judicial, se identifican las siguientes categorías de herramientas y código malicioso empleados por los adversarios:

- **Motores de Cifrado y Ransomware de Impacto Sistémico:** Artefactos de software malicioso diseñados con algoritmos de cifrado de alta velocidad que apuntan directamente a los repositorios de datos centralizados. Estas herramientas son las responsables directas de los incidentes de denegación de servicio internos, logrando comprometer la disponibilidad de las aplicaciones misionales, deshabilitar los portales de consulta ciudadana y forzar la suspensión temporal de los servicios digitales en dependencias críticas como la Justicia Penal Militar y Policial.

- **Cargadores Avanzados (Loaders) e Implantes SHA-256:** Código compilado de última generación que se detecta en la telemetría a través de 142 firmas únicas.

El propósito principal de estas herramientas es actuar como la primera etapa de ejecución en las estaciones de trabajo de los funcionarios judiciales; cuentan con capacidades de evasión de defensas integradas que les permiten burlar las soluciones antivirus tradicionales (EDR/AV) y facilitar la inyección silenciosa de payloads secundarios en la memoria del sistema.

- **Herramientas de Intrusión Estándar y Scripts Reutilizados (SHA-1 / MD5):** Componentes técnicos secundarios y utilidades de administración de red legítimas que han sido modificadas o abusadas por los atacantes (Dual-Use Tools). Identificadas a través de 272 huellas criptográficas en las plataformas TIP, estas herramientas automatizadas se emplean para la ejecución de scripts de explotación local, escaneo interno de redes de los tribunales y recolección rápida de metadatos del sistema informático comprometido.

- **Kits de Phishing y Frameworks de Suplantación Web:** Software especializado en el despliegue automatizado de interfaces gráficas que clonan con precisión los portales oficiales de autenticación judicial y sistemas de correo del Estado. Apoyados en la infraestructura dinámica de más de 2,200 nombres de dominio (FQDN), estos kits operan como herramientas de recolección masiva de credenciales y tokens de acceso de usuarios legítimos de la rama.

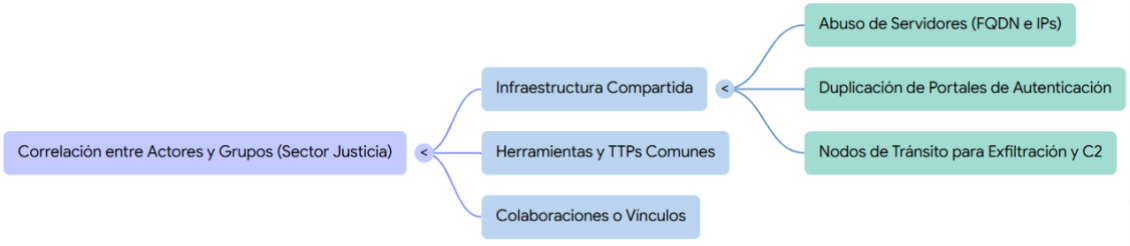
- **Troyanos de Acceso Remoto (RATs) y Canales C2:** Implantes maliciosos programados para establecer conexiones salientes ocultas hacia la red de 754 direcciones IP controladas por los adversarios. Estas herramientas permiten a los operadores remotos ejecutar comandos en tiempo real, realizar movimientos laterales dentro de las redes territoriales del sector justicia y asegurar la persistencia en el entorno sin interactuar directamente con los perímetros de seguridad más vigilados.

CORRELACIÓN ENTRE ACTORES Y GRUPOS

El análisis estratégico de la telemetría unificada en las herramientas TIP revela una correlación directa entre la infraestructura maliciosa desplegada y el nivel de sofisticación de los atacantes que amenazan al sector Justicia. La concentración de los 3,407 indicadores de compromiso en un conjunto definido de 11 actores de amenazas avanzadas persistentes (APTs) y células de cibercrimen demuestra que las agresiones no corresponden a eventos aislados, sino a campañas corporativas planificadas.

En este ecosistema, los grupos de ransomware explotan sistemas vulnerables para paralizar la continuidad de servicios digitales esenciales —como los de la Justicia Penal Militar—, mientras que los actores de espionaje coordinan el uso masivo de nombres de dominio (FQDN) y el secuestro de cuentas con privilegios territoriales para infiltrarse de manera silenciosa, permitiendo vincular de forma inequívoca el tipo de componente tecnológico detectado en el perímetro con los objetivos estratégicos de cada grupo delictivo.

Infraestructura Compartida

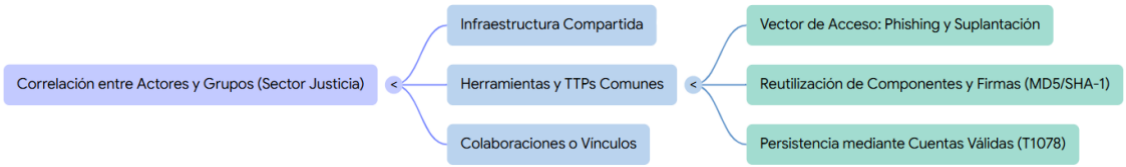


- **Abuso Centralizado de Servidores de Red (FQDN e IPs):** Los atacantes concentran la administración de sus operaciones en una base común de servidores de alojamiento. Esto se evidencia en la correlación de los 2,205 nombres de dominio (FQDN) y 754 direcciones IP activos que sirven de soporte simultáneo tanto para campañas de espionaje como para los preparativos de intrusiones de ransomware de los grupos bajo monitoreo.

- **Duplicación de Portales de Autenticación Judicial:** Se observa el uso de los mismos bloques de infraestructura dinámica de red para alojar páginas web fraudulentas que clonan de manera idéntica las interfaces de acceso institucional. Estas plantillas y servidores de captura son explotados por distintos operadores para comprometer de forma masiva cuentas de usuarios con privilegios en la rama.

- **Nodos de Tránsito para Exfiltración y C2:** Las direcciones IP identificadas operan como pasarelas de comunicación compartidas. Varios grupos delictivos direccionan el tráfico de sus troyanos de acceso remoto (RATs) hacia estos mismos nodos de enrutamiento malicioso para coordinar la descarga de payloads o centralizar la extracción silenciosa de expedientes procesales.

Herramientas y TTPs Comunes

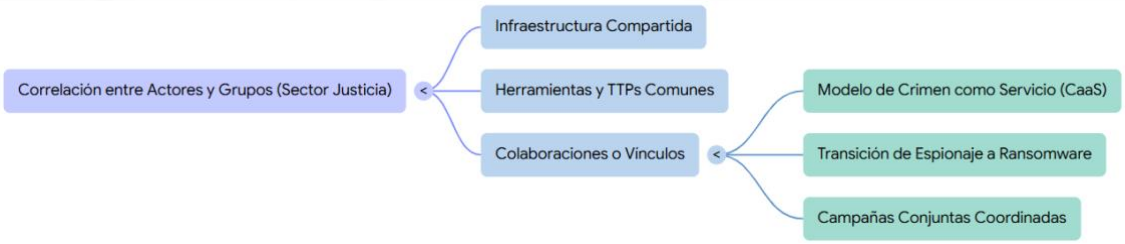


- **Estandarización en el Vector de Acceso (Phishing y Suplantación):** Todos los actores correlacionados emplean de manera recurrente la táctica de Acceso Inicial mediante Phishing (T1566) apoyados en técnicas de Enmascaramiento (T1036). Esta uniformidad metodológica demuestra que la suplantación de la identidad digital del Estado es el procedimiento estándar para vulnerar el sector.

- **Reutilización de Componentes y Scripts (SHA-1 / MD5):** Se identifica el uso constante de un mismo conjunto de herramientas de intrusión secundarias, utilidades de administración modificadas (*Dual-Use Tools*) y scripts de explotación local. Este arsenal genérico se ve reflejado en la simetría matemática de las 272 firmas criptográficas MD5 y SHA-1 presentes en la telemetría global del sector.

- **Persistencia mediante Abuso de Cuentas Válidas:** Una vez obtenidas las credenciales legítimas de los funcionarios en los entornos territoriales, los adversarios aplican de manera unánime la técnica de Cuentas Válidas (T1078). Este procedimiento común les permite evadir las alarmas tradicionales e inspeccionar los repositorios centrales sin necesidad de desplegar exploits de día cero.

Posibles Colaboraciones o Vínculos



- **Modelo Operativo de Crimen como Servicio (CaaS):** Los datos sugieren la existencia de alianzas estratégicas donde intermediarios de acceso inicial (IABs) comprometen los perímetros de la rama judicial o recolectan las credenciales para, posteriormente, transferir o vender este control operativo a los 11 grupos APT o bandas de ransomware monitoreadas.

- **Transición del Espionaje a la Denegación de Servicio:** El entrelazamiento de las herramientas de acceso (kits de phishing/dominios) con las de impacto (motores de cifrado) evidencia un vínculo logístico. Intrusiones que inicialmente muestran un comportamiento de extracción silenciosa de información procesal terminan sirviendo como puente técnico para el despliegue de ataques de ransomware.

- **Campañas Conjuntas Contra la Infraestructura Estatal:** Los grupos de ransomware coordinan sus ofensivas para golpear de forma simultánea múltiples dependencias estatales transversales y portales judiciales. Este comportamiento coordinado confirma que los atacantes comparten inteligencia sobre las debilidades del sector público para potenciar el impacto sistémico y maximizar la efectividad de sus extorsiones económicas en eventos como los sufridos por la Justicia Penal Militar.

Visualización de Relaciones

Para comprender con precisión el engranaje operativo de las amenazas que asedian al sector, es fundamental analizar cómo interactúan los componentes técnicos con los objetivos estratégicos de los atacantes. La siguiente representación gráfica desglosa de manera relacional el flujo de las campañas identificadas, vinculando el origen de la telemetría multi-fuente, la centralización de la infraestructura compartida por los 11 actores avanzados (APTs), y la ejecución secuencial de sus tácticas según el marco MITRE ATT&CK.

Este mapeo visual permite rastrear cómo un indicador atómico perimetral —como un nombre de dominio (FQDN) o una dirección IP— se transforma en un vector de acceso inicial o un implante de evasión, guiando de forma directa la toma de decisiones para la protección de expedientes reservados y la continuidad de los servicios digitales esenciales de la rama judicial.

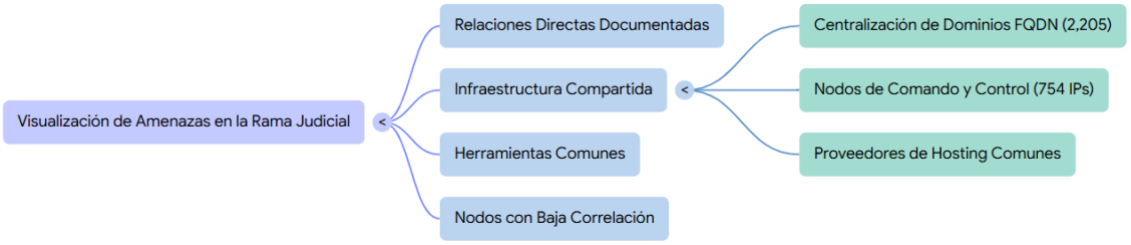
Relaciones directas documentadas:

- **Vinculación Actor-Objetivo en la Rama Judicial:** Existen registros explícitos que asocian las campañas de los 11 actores APT con el interés directo de comprometer expedientes bajo reserva legal y repositorios institucionales de consulta procesal pública.

- **Ataques de Ransomware Confirmados a Servicios Críticos:** Se encuentra plenamente documentado el nexo causal entre las células de cibercrimen extorsivo y la parálisis operativa total sufrida en los servicios electrónicos y canales digitales de dependencias clave como la Justicia Penal Militar y Policial.

- **Campañas de Phishing Focalizadas contra Funcionarios:** Relación directa comprobada entre el envío de correos fraudulentos a las bandejas institucionales de magistrados o jueces y el posterior robo masivo de credenciales de acceso con privilegios de administración territorial.

Relaciones por infraestructura compartida

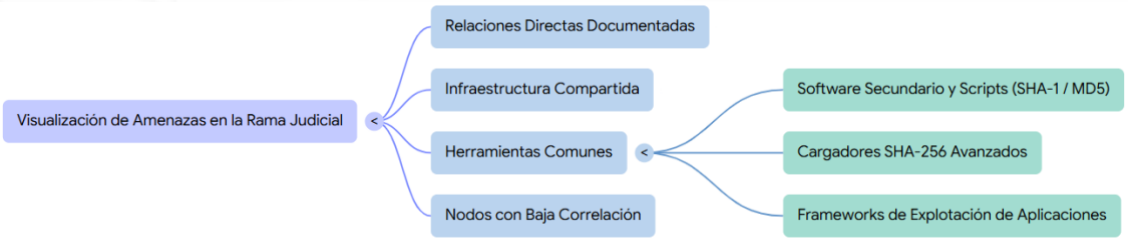


- **Centralización de Servidores en Bloques FQDN:** Correlación técnica en la que diversos grupos de amenazas utilizan de forma simultánea o secuencial los mismos 2,205 nombres de dominio dinámicos para simular portales del Estado y desplegar interfaces de suplantación.

- **Coincidencia en Nodos de Comando y Control (C2):** Mapeo de múltiples cepas de malware independientes que dirigen su tráfico de exfiltración y reciben instrucciones remotas desde el mismo bloque consolidado de 754 direcciones IP maliciosas.

- **Uso de Proveedores Comunes de Hosting Evade-Bloqueos:** Evidencia de que tanto los actores avanzados de espionaje como los operadores de ransomware adquieren servicios en los mismos servidores de alojamiento globales para desplegar sus implantes de red contra el ecosistema judicial colombiano.

Relaciones por herramientas comunes

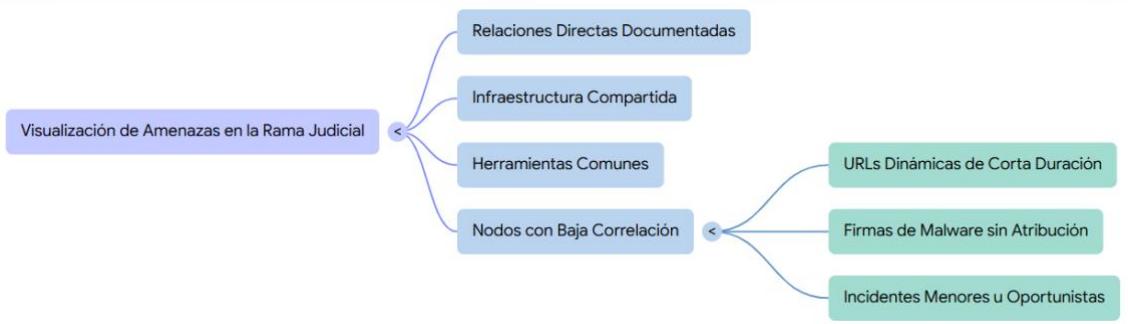


- **Homogeneidad en Software Secundario y Scripts (SHA-1 / MD5):** Identificación de patrones idénticos en el uso de utilidades de intrusión de doble uso (*Dual-Use Tools*) y scripts de automatización local, reflejados simétricamente en las 272 firmas criptográficas antiguas procesadas en las plataformas TIP.

- **Estandarización de Cargadores Avanzados (SHA-256):** Adopción transversal de las mismas tecnologías de evasión perimetral por parte de los atacantes, quienes comparten estructuras de código en 142 cargadores modernos para neutralizar de forma uniforme las soluciones antivirus locales.

- **Uso Compartido de Frameworks de Explotación de Aplicaciones:** Empleo de metodologías y kits de explotación comunes para detectar y vulnerar de manera idéntica fallas en portales web y servicios estatales expuestos en el perímetro nacional.

Nodos aislados o con baja correlación (por ahora):



- **Enlaces Web Específicos de Corta Duración (URLs):** Los 34 indicadores basados en URLs puntuales presentan una correlación extremadamente baja, debido a que son enlaces dinámicos generados para un único desvío o campaña de phishing de un solo uso que se inactivan rápidamente.

- **Firmas de Malware Huérfanas de Actor Autor:** Un porcentaje menor de huellas criptográficas SHA-256 detectadas localmente en estaciones territoriales aún no han podido ser atribuidas formalmente a ninguno de los 11 actores APT principales bajo monitoreo en el TIP.

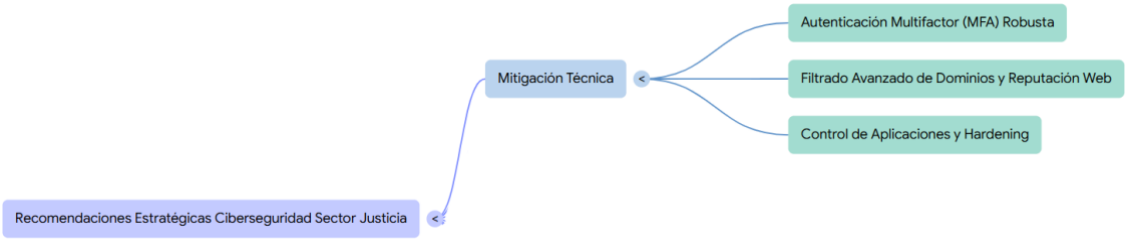
- **Incidentes Menores o Intrusiones Oportunistas:** Registros aislados de escaneos aleatorios de puertos y denegaciones de servicio menores en páginas web de juzgados locales que, de momento, corresponden a ciberdelincuencia común o *script kiddies* sin vínculos con las campañas dirigidas de alto impacto.

RECOMENDACIONES ESTRATÉGICAS

El panorama de amenazas identificado para el sector Justicia en Colombia exige la transición de un modelo de seguridad reactivo hacia una postura de defensa proactiva y unificada. Ante el despliegue sistemático de infraestructura de red fraudulenta y campañas avanzadas de ransomware dirigidas a la parálisis de los servicios públicos, es imperativo establecer un marco de recomendaciones estratégicas que fortalezca los controles técnicos, optimice las capacidades de visibilidad en tiempo real y asegure la continuidad de la administración de la ley frente a incidentes de alto impacto.

Recomendaciones de Mitigación Técnica

Para contrarrestar de forma directa el vector de acceso predominante y la descarga de componentes maliciosos, las instituciones de la rama judicial deben robustecer las capacidades de sus controles perimetrales y de punto final (endpoint), cerrando las brechas operativas que explotan los adversarios.



- **Implementación de Autenticación Multifactor (MFA) Robusta:** Desplegar de manera obligatoria esquemas de MFA para el acceso a correos institucionales, sistemas de radicación de demandas y portales de gestión procesal, mitigando el riesgo de compromiso de cuentas mediante credenciales obtenidas en portales falsos de suplantación web.
- **Filtrado Avanzado de Dominios y Reputación Web:** Configurar políticas restrictivas en los firewalls perimetrales y servidores proxy para bloquear de forma automatizada las conexiones dirigidas hacia nombres de dominio de reciente creación, DNS dinámicos o la lista de FQDN maliciosos identificados en las plataformas TIP.
- **Políticas de Control de Aplicaciones y Endurecimiento (Hardening):** Restringir la ejecución de scripts no autorizados (PowerShell, VBScript) y herramientas de doble uso (*Dual-Use Tools*) en las estaciones territoriales, bloqueando los vectores comunes de cargadores avanzados (SHA-256) y componentes de intrusión genéricos (SHA-1/MD5).

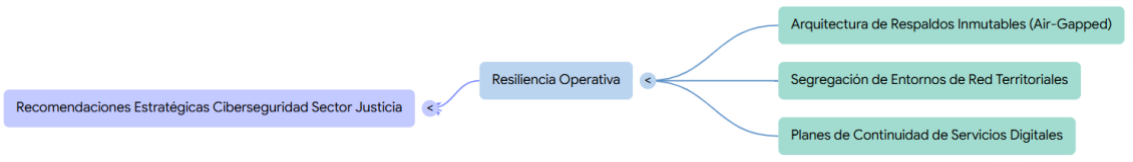
Recomendaciones de Detección y Monitoreo

La visibilidad oportuna de la telemetría es fundamental para neutralizar las campañas de espionaje y los movimientos laterales antes de que comprometan los servidores centrales; por ello, se debe potenciar la capacidad de detección analítica del Centro de Operaciones de Seguridad (SOC).

- **Correlación Dinámica de Eventos de Capa de Aplicación:** Desarrollar reglas de correlación específicas en el SIEM para monitorear patrones de tráfico HTTP/HTTPS inusuales dirigidos hacia el bloque de direcciones IP identificadas como Comando y Control (C2), detectando conexiones salientes anómalas desde los servidores de la rama.
- **Despliegue Homogéneo de Soluciones EDR:** Asegurar la cobertura total de agentes de Detección y Respuesta en Endpoints (EDR) en los equipos de funcionarios y magistrados a nivel nacional, configurando alertas basadas en el comportamiento para identificar el uso de técnicas MITRE ATT&CK como Phishing (T1566) y Enmascaramiento (T1036).
- **Ingesta Automatizada de Ciberinteligencia (Threat Intelligence):** Sincronizar de forma continua los feeds de las plataformas de inteligencia (incluyendo *Google Threat Intelligence*, comunidades sectoriales y *MISP Import*) con las herramientas de detección perimetral para aplicar bloqueos predictivos basados en nuevos indicadores atómicos cargados.

Recomendaciones de Resiliencia Operativa

Dado que las bandas de ransomware dirigen sus esfuerzos a quebrantar la disponibilidad de la infraestructura crítica, la rama judicial debe garantizar que sus procesos misionales sobrevivan a un compromiso técnico profundo en sus redes.



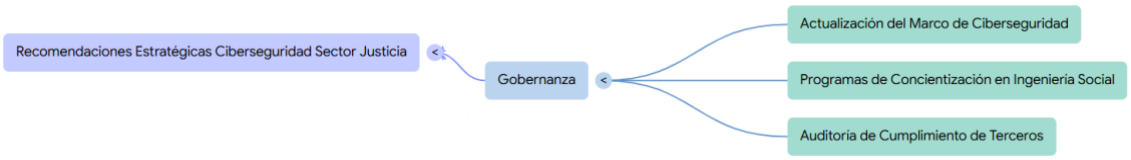
- **Arquitectura de Respaldos Inmutables y Desconectados (Air-Gapped):** Establecer políticas de copias de seguridad periódicas para expedientes

judiciales y bases de datos centralizadas, asegurando que los respaldos críticos se almacenen de forma cifrada, aislada de la red principal e inaccesible para los motores de cifrado maliciosos.

- **Segregación de Entornos de Red Territoriales:** Segmentar de forma estricta las redes de los tribunales y dependencias locales respecto a los servidores de datos centrales, impidiendo que el compromiso de una cuenta o terminal en un nodo periférico facilite el movimiento lateral hacia aplicaciones transversales del Estado.
- **Planes de Continuidad de Servicios Digitales:** Diseñar esquemas alternativos de contingencia operativa y procesamiento manual temporal que permitan mantener los canales de atención al ciudadano y las consultas procesales básicas ante escenarios de parálisis de portales institucionales.

Recomendaciones de Gobernanza

La efectividad de la seguridad técnica depende de un marco normativo interno sólido, liderado por el Ministerio de Justicia y del Derecho, que estandarice las responsabilidades y supervise el cumplimiento de las políticas de protección de datos.



- **Actualización del Marco de Ciberseguridad Institucional:** Revisar y alinear las directrices de seguridad de la información con las amenazas activas del sector público, formalizando manuales que obliguen a todas las dependencias judiciales a auditar periódicamente sus sistemas expuestos.
- **Programas de Concientización en Ingeniería Social:** Implementar campañas continuas de capacitación y simulacros de phishing enfocados en el personal administrativo y funcionarios judiciales, reduciendo la tasa de éxito de los atacantes que emplean tácticas de suplantación de identidad digital del Estado.
- **Auditoría de Cumplimiento de Terceros y Proveedores:** Establecer cláusulas estrictas de seguridad digital para contratistas y proveedores tecnológicos que administran portales web de la rama, garantizando que sus accesos y plataformas cumplan con los mismos estándares de mitigación exigidos a las entidades internas.

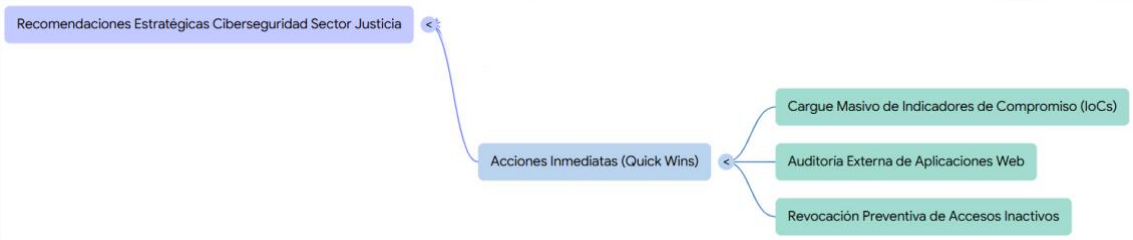
Preparación ante Incidentes

La respuesta oportuna frente a incidentes críticos, como los ataques evidenciados en la Justicia Penal Militar, requiere una estructura de mando coordinada y protocolos preestablecidos para contener los daños rápidamente.

- **Creación de Playbooks Específicos contra Ransomware y Fuga de Datos:** Desarrollar guías técnicas de respuesta paso a paso que definan las acciones inmediatas de aislamiento de redes, contención de credenciales comprometidas y preservación de evidencia forense digital ante intrusiones confirmadas.
- **Ejercicios de Simulación de Crisis (Tabletop Executivos):** Realizar simulaciones periódicas con la alta dirección de la rama judicial para ensayar la toma de decisiones estratégicas, los canales de comunicación legal y los mecanismos de notificación ante secuestros masivos de activos de información.
- **Canales Integrados de Comunicación Sectorial:** Estrechar los lazos de cooperación técnica con los CSIRT nacionales y gubernamentales para agilizar el intercambio de Indicadores de Compromiso (IoCs) frescos detectados localmente, permitiendo alertar preventivamente a otras entidades del sector público.

Acciones Inmediatas (Quick Wins)

Estas medidas de rápida ejecución y bajo costo operativo permiten elevar de forma inmediata el nivel de seguridad perimetral mientras se despliegan los proyectos estratégicos de mediano plazo.



- **Cargue Masivo de Indicadores de Compromiso en Pasarelas de Seguridad:** Importar de forma inmediata el universo de los 3,407 IOCs procesados (los 2,205 dominios FQDN, las 754 direcciones IP y las firmas criptográficas de malware) directamente en las reglas de bloqueo de los firewalls, proxies y antivirus institucionales.
- **Auditoría Externa de Aplicaciones Web Expuestas:** Ejecutar un escaneo prioritario de vulnerabilidades sobre los portales de consulta judicial y sistemas de radicación electrónica para parchar fallas críticas expuestas a internet que puedan ser explotadas para accesos iniciales oportunistas.
- **Revocación Preventiva de Accesos Inactivos o Anómalos:** Realizar una depuración urgente de las cuentas de usuario y credenciales con privilegios administrativos a nivel territorial, deshabilitando accesos de exfuncionarios o cuentas sin uso registrado para mitigar la técnica de Cuentas Válidas.

CONCLUSIONES

1. **Predominio táctico de operaciones en el plano de red:** El análisis cuantitativo demuestra de forma contundente que la infraestructura adversaria se concentra en vectores de red, donde un 64.7% de los 3,407 indicadores corresponde a nombres de dominio (2,205 FQDN) y un 22.1% a direcciones IP (754 registros). Esta asimetría cuantitativa confirma que el esfuerzo principal de los atacantes se enfoca en el enmascaramiento de servidores de Comando y Control (C2) y en la creación de portales de suplantación de identidad para el robo de accesos institucionales.

2. **Sofisticación y modularidad en el despliegue de malware:** La distribución equilibrada y simétrica de las huellas criptográficas de archivos (142 hashes SHA-256, 136 SHA-1 y 136 MD5) evidencia una metodología de intrusión corporativa y modular. Los atacantes entrelazan de forma estratégica cargadores e implantes de última generación (SHA-256) para evadir soluciones antivirus tradicionales con librerías de soporte técnico y scripts automatizados reutilizados (SHA-1/MD5) para afianzar su persistencia en los servidores.

3. **Focalización del riesgo por amenazas persistentes dirigidas:** El ecosistema digital de la rama judicial no experimenta agresiones oportunistas o aleatorias, sino campañas estructuradas y coordinadas por un núcleo definido de 11 actores avanzados de amenazas (APTs y grupos UNC) bajo monitoreo en las herramientas TIP. Estos grupos sostienen un interés estratégico permanente enfocado en el

ciberespionaje, la manipulación de bases de datos de alta confidencialidad y la exfiltración silenciosa de expedientes bajo reserva legal.

4. **Elevado impacto y vulnerabilidad real ante el cibercrimen financiero:** Los antecedentes históricos del sector —como el secuestro de portales que afectó a decenas de webs estatales en 2023 y la parálisis perimetral sufrida por la Justicia Penal Militar y Policial en 2025— comprueban que el ransomware representa un riesgo de criticidad operativa inmediata. Las bandas delictivas poseen la capacidad demostrada de interrumpir la disponibilidad de las herramientas misionales del Estado, usándolas como mecanismo de presión extorsiva nacional.

5. **Evasión avanzada mediante el abuso de infraestructuras legítimas:** Las puntuaciones de riesgo más severas dentro de la escala TIP (calificaciones de 18 a 20) se asocian al uso deliberado de servicios legítimos de almacenamiento en la nube comercial y túneles automatizados. Al alojar sus payloads y componentes dañinos en dominios de alta reputación y restringir el uso de URLs estáticas explícitas (solo 34 registros), los adversarios mitigan la efectividad de las cajas de arena (*sandboxing*) y los filtros de contenido tradicionales.

6. **Ampliación crítica de la superficie de ataque por la digitalización:** El paso acelerado hacia la justicia electrónica, la adopción de audiencias virtuales, la interconexión de sedes territoriales y la habilitación de portales web de radicación ciudadana han expandido drásticamente el perímetro expuesto de la rama. Esta densa red de activos e interconexiones institucionales es monitorizada constantemente por los adversarios, quienes buscan vulnerabilidades tanto en el software expuesto a Internet como en los privilegios de los accesos de los usuarios legítimos.

7. **Necesidad imperativa de una defensa proactiva y validada:** El respaldo analítico del 100% de los indicadores procesados a través de redes globales de confianza (como el ecosistema de *Google Threat Intelligence* y plataformas comunitarias como MISP) ratifica la veracidad y vigencia de las amenazas mapeadas. Para salvaguardar la soberanía jurídica digital de la Nación, es indispensable abandonar los esquemas defensivos estáticos tradicionales y migrar con urgencia hacia un modelo basado en la autenticación robusta, la segmentación rigurosa de redes de expedientes y el monitoreo adaptativo en tiempo real.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **Plataforma de Inteligencia de Amenazas (TIP - Threat Intelligence Platform):** Sistema tecnológico utilizado para recopilar, agregar, correlacionar y analizar datos sobre amenazas cibernéticas globales procedentes de múltiples fuentes. En el informe, facilita la centralización y validación cruzada de los 3,407 indicadores detectados.

- **Indicador de Compromiso (IoC - Indicator of Compromise):** Evidencia forense digital o rastro técnico (como un dominio, una IP o una firma de archivo) que indica con un alto grado de certeza que un sistema informático ha sido vulnerado o que existe una actividad maliciosa en curso.

- **Amenaza Avanzada Persistente (APT - Advanced Persistent Threat):** Grupo de ciberoperadores altamente capacitados y financiados (frecuentemente vinculados a estados o gobiernos) que ejecutan campañas de intrusión dirigidas, prolongadas y sigilosas. El informe monitorea a 11 de estos adversarios orientados al ciberespionaje.

- **Grupos UNC (Uncategorized):** Denominación temporal que otorgan las firmas de ciberinteligencia a un conjunto de actividades maliciosas o a un grupo de atacantes que aún no ha sido clasificado formalmente bajo un nombre definitivo (como un número APT o FIN), pero que comparte tácticas y patrones comunes.

- **Ciberespionaje:** Operaciones encubiertas en el ciberespacio destinadas a interceptar comunicaciones, comprometer credenciales y exfiltrar de manera silenciosa activos de información sensible (como expedientes bajo reserva legal o estrategias de defensa) sin alterar los sistemas infectados.

- **Phishing:** Vector de acceso inicial basado en técnicas de ingeniería social, mediante el cual los atacantes envían correos electrónicos fraudulentos simulando ser entidades legítimas del Estado para engañar a los funcionarios y capturar sus credenciales de acceso.

Infraestructura y Redes

- **Nombre de Dominio Completamente Calificado (FQDN - Fully Qualified Domain Name):** Dirección de red única y completa en Internet que identifica de forma exacta a un servidor (ej. un portal judicial clonado). Representa el 64.7% del total de las amenazas analizadas (2,205 registros).

- **Dirección IP (Internet Protocol):** Identificador numérico asignado a cada dispositivo conectado a una red informática. En este informe se identificaron 754 IPs que corresponden a servidores legítimos comprometidos globalmente o infraestructuras en la nube elástica controladas por los atacantes.

- **Mando y Control (C2 - Command and Control):** Infraestructura de servidores web y de red que utilizan los adversarios para enviar órdenes de ejecución, configurar persistencias y recibir de vuelta la información exfiltrada desde los sistemas internos secuestrados.

- **Superficie de Ataque:** La suma total de puntos de exposición, activos tecnológicos, portales públicos, estaciones de trabajo y servicios en la nube a través de los cuales un atacante puede intentar introducirse a las redes de la rama judicial.

- **Segmentación de Red:** Práctica de arquitectura de seguridad que consiste en dividir una red informática en subredes más pequeñas y aisladas entre sí. Impide el movimiento lateral de un malware si una estación periférica resulta comprometida.

- **Autenticación Multifactor (MFA):** Control de identidad que exige a los usuarios suministrar dos o más evidencias diferentes para conceder el acceso a una cuenta (ej. una contraseña y un código token dinámico), neutralizando el uso de credenciales robadas mediante phishing.

Herramientas y Malware

- **Ransomware:** Tipo de código malicioso diseñado para bloquear el acceso a los sistemas informáticos o cifrar de forma masiva bases de datos y archivos institucionales. Los atacantes exigen un pago económico (extorsión) a cambio de la clave de descifrado, paralizando servicios como los portales de consulta ciudadana.

- **Malware Modular:** Software dañino estructurado en diferentes componentes o "módulos" independientes. Esto permite a los atacantes modificar sus capacidades en tiempo real (añadir funciones de espionaje, robo de contraseñas o destrucción) según el entorno infectado.

- **Hash Criptográfico (SHA-256, SHA-1, MD5):** Huella digital o firma criptográfica única generada a partir de un archivo informático. Permite a las soluciones de seguridad identificar de forma matemática y exacta si un ejecutable o script coincide con un código malicioso previamente registrado a nivel internacional.

- **Cargador de Malware (Loader):** Tipo de software malicioso intermedio diseñado específicamente para evadir las defensas perimetrales e inyectar de manera silenciosa en la memoria del sistema las cargas dañinas o payloads de segunda etapa.

- **Payload (Carga Útil):** El componente del código malicioso que ejecuta la acción dañina principal programada por el atacante, tal como la exfiltración de expedientes confidenciales o la activación del cifrado de datos.

Sector Justicia

- **Rama Judicial de Colombia:** Poder público del Estado encargado de administrar justicia, resolver litigios entre ciudadanos o entre estos y el Estado, y garantizar el cumplimiento de los derechos y libertades. Está integrada por las altas cortes, juzgados de circuito, tribunales territoriales y la fiscalía general de la Nación.

- **Justicia Digital (Justicia Electrónica):** Proceso de transformación tecnológica e institucional enfocado en migrar los trámites legales tradicionales hacia entornos electrónicos, abarcando portales de radicación de demandas, audiencias virtuales y la digitalización de los procesos judiciales.

- **Expediente Digital:** Conjunto organizado de documentos electrónicos, actuaciones procesales, pruebas y registros multimedia que conforman un caso judicial. Su confidencialidad e integridad son críticas, ya que contienen datos sensibles de investigaciones en curso, testigos protegidos o estrategias legales del Estado.

- **Justicia Penal Militar y Policial:** Dependencia especializada encargada de la investigación y juzgamiento de las conductas punibles cometidas por los miembros de la Fuerza Pública en servicio activo. Es catalogada como un blanco de alto impacto técnico tras sufrir incidentes que forzaron la suspensión temporal de sus portales y canales electrónicos misionales.

- **Soberanía Jurídica Digital:** Capacidad y derecho autónomo del Estado para garantizar el control total, la protección irrestricta y la reserva absoluta sobre sus

datos procesales, plataformas de litigio nacional y expedientes de alta sensibilidad frente a interferencias o secuestros cibernéticos transnacionales.

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