TIC

Informe de apreciación Sector

Educación

COLCERT

Contenido

Informe de apreciación
Sector Educación

COLCERT IN-20260704-035

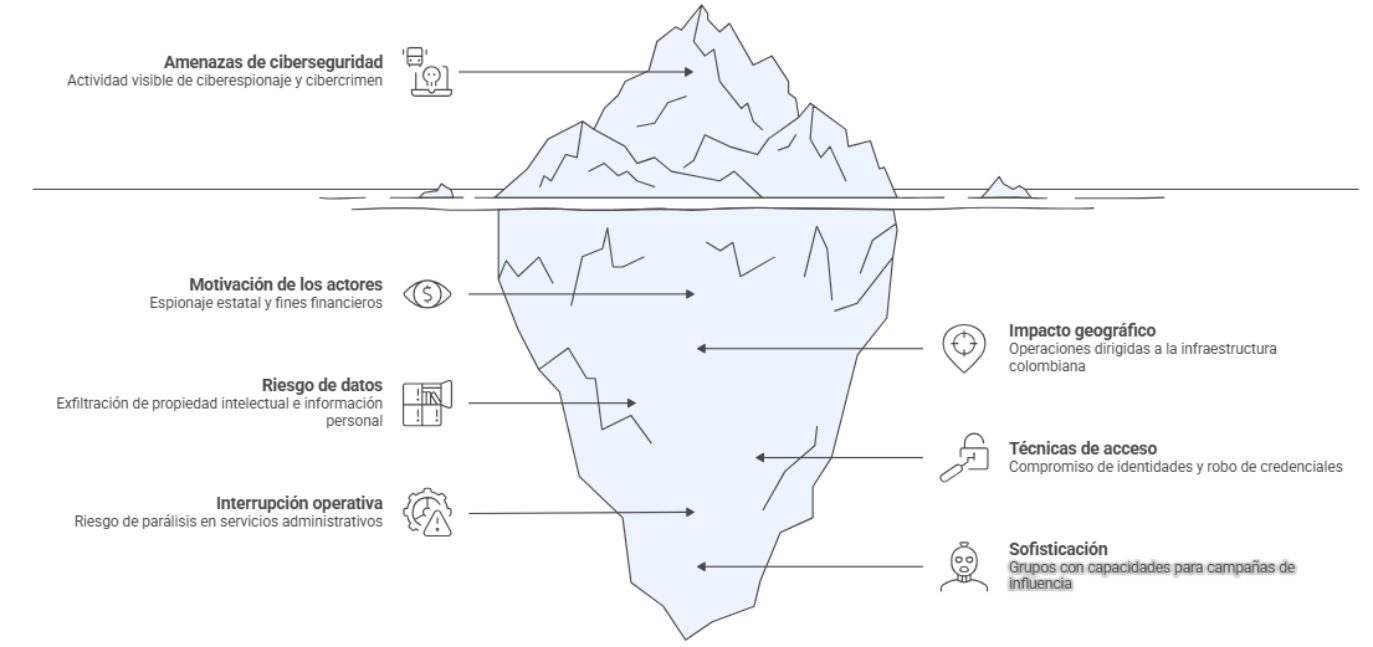
TLP: CLEAR

INTRODUCCIÓN

El sector educativo en Colombia se ha consolidado como un activo estratégico de alto valor, albergando no solo la formación del capital humano del país, sino también investigaciones críticas y vastas bases de datos personales. Esta concentración de información sensible, sumada a la apertura tecnológica necesaria para el entorno académico, ha generado una superficie de exposición aprovechada por actores con motivaciones diversas. El presente documento detalla el estado actual de las amenazas, analizando el comportamiento de grupos que buscan desde la exfiltración de propiedad intelectual hasta el beneficio económico mediante la interrupción operativa, con el fin de establecer una postura defensiva sólida y resiliente.

Lineamientos

- Confidencialidad en el manejo de la información técnica.
- Priorización de la protección de la identidad académica.
- Enfoque en la resiliencia de la infraestructura crítica de investigación.
- Cumplimiento de las normativas nacionales de protección de datos personales.
- Mitigación proactiva basada en indicadores de compromiso locales.
- Alineación con los estándares de ciberseguridad nacional para el sector público y privado.



Informe de apreciación
Sector Educación

COLCERT IN-20260704-035

TLP: CLEAR

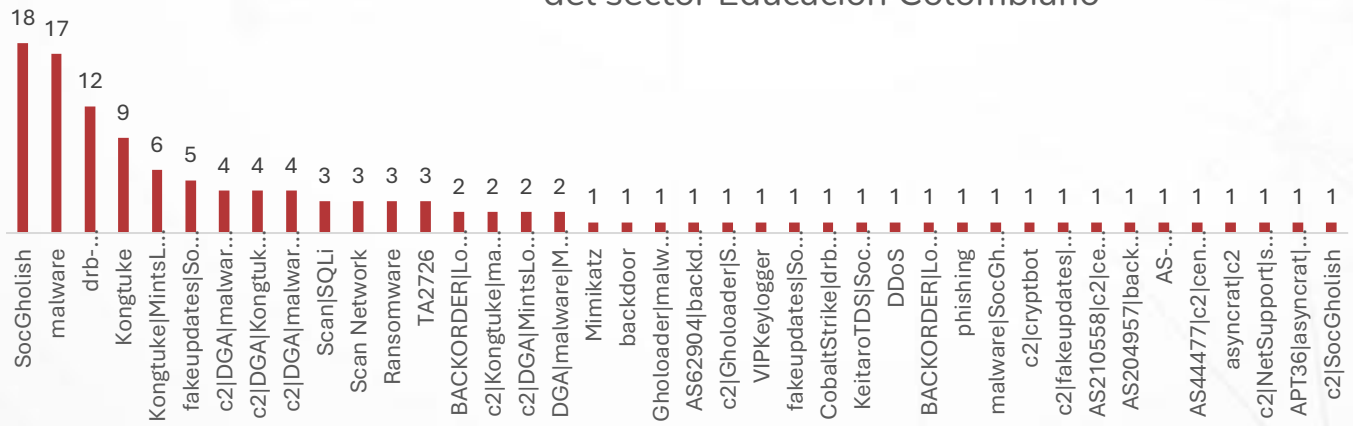
RESUMEN EJECUTIVO

El panorama de amenazas para el sector educativo en Colombia durante el periodo actual muestra una actividad persistente de grupos de ciberespionaje y cibercrimen organizado con motivaciones financieras. Las instituciones educativas, que gestionan grandes volúmenes de datos personales, propiedad intelectual e investigaciones críticas, son objetivos estratégicos para actores que buscan tanto el beneficio económico como la exfiltración de información sensible. La presencia de actores vinculados a campañas de influencia y robo de credenciales subraya la necesidad de fortalecer la resuelta de las infraestructuras académicas frente a incidentes de alto impacto.

Aspectos clave:

- *Motivación de los actores:* Mezcla de espionaje estatal y fines financieros.
- *Impacto geográfico:* Operaciones dirigidas específicamente a la infraestructura en Colombia.
- *Riesgo de datos:* Exfiltración de propiedad intelectual e información personal académica.
- *Técnicas de acceso:* Compromiso de identidades y robo de credenciales de la comunidad educativa.
- *Interrupción operativa:* Riesgo de parálisis en servicios administrativos y financieros.
- *Sofisticación:* Presencia de grupos con capacidades para campañas de influencia y desinformación.

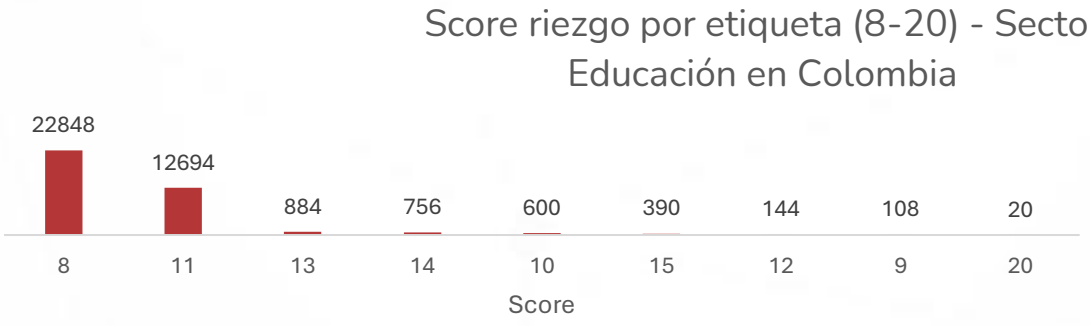
Malware actores C2 identificados: insumos para la ciberseguridad del sector Educación Colombiano



Hallazgos Clave

Hallazgos Clave

- Diversidad de Actores: Se identifica la actividad de grupos especializados en el robo de propiedad intelectual y campañas de desinformación, con una presencia notable de adversarios que operan a nivel global y han puesto su foco en objetivos colombianos.
- Interés en Credenciales y Acceso: Existe una tendencia marcada hacia el uso de técnicas de acceso inicial que comprometen la identidad de estudiantes y docentes para infiltrarse en redes institucionales.
- Presencia de Amenazas Financieras: Grupos enfocados en el fraude y el movimiento lateral dentro de redes corporativas han sido detectados operando en la región, lo que aumenta el riesgo de incidentes relacionados con la interrupción de servicios administrativos.



Recomendaciones Prioritarias

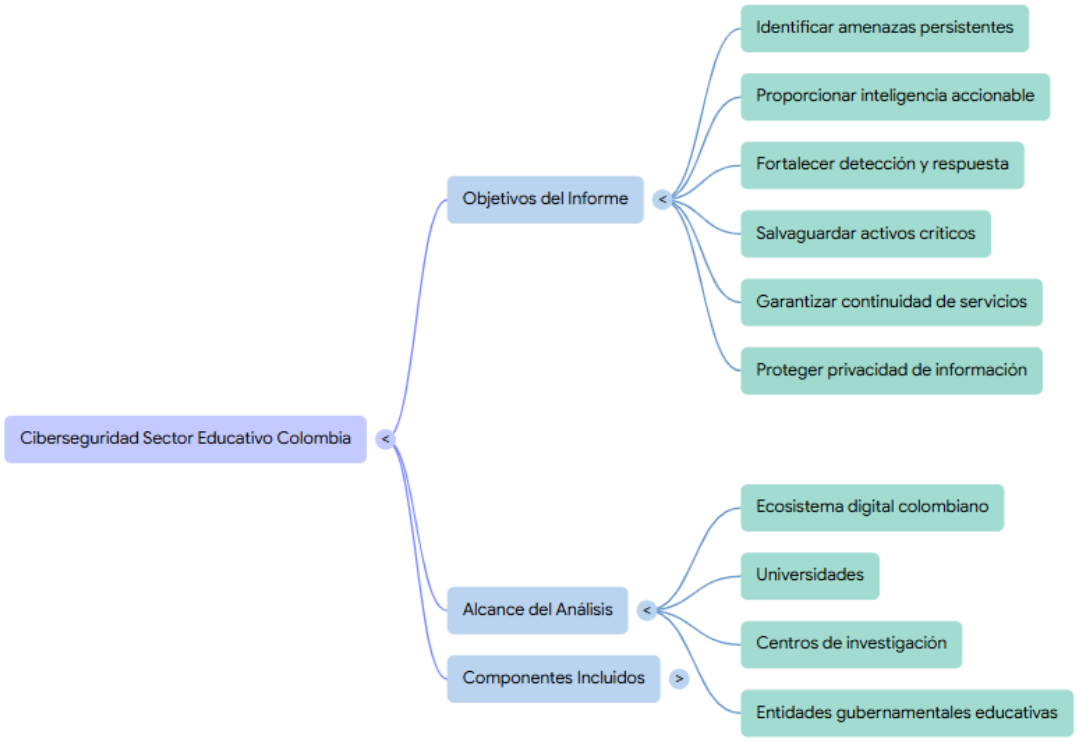
- Fortalecimiento de la Identidad: Implementar mecanismos robustos de verificación para todos los usuarios que acceden a servicios académicos y plataformas de investigación.
- Segmentación de Redes Académicas: Separar los entornos de laboratorios y uso estudiantil de los sistemas críticos de administración y bases de datos de investigación.

- Monitoreo de Exfiltración: Establecer controles estrictos sobre la salida de datos para detectar volúmenes inusuales de información que sugieran un compromiso de propiedad intelectual.

Conclusión Estratégica

El sector educación debe evolucionar de un enfoque de conectividad abierta hacia uno de seguridad proactiva. La madurez cibernética en este sector es fundamental no solo para proteger la operatividad diaria, sino para salvaguardar el capital intelectual del país y la privacidad de su comunidad académica frente a adversarios externos altamente capacitados.

OBJETIVO Y ALCANCE



Informe de apreciación
Sector Educación

COLCERT IN-20260704-035

TLP: CLEAR

Objetivo

El presente informe tiene como propósito fundamental identificar y desglosar las amenazas persistentes que impactan la infraestructura tecnológica del sector educativo en Colombia. A través del análisis de los actores con actividad reciente en el país, se busca proporcionar inteligencia accionable que permita fortalecer las capacidades de detección y respuesta de las instituciones académicas. El objetivo final es salvaguardar la integridad de los activos críticos, la continuidad de los servicios educativos y la privacidad de la información sensible frente a operaciones de espionaje y cibercrimen organizado.

Alcance

El análisis detallado en este documento se circunscribe a la evaluación de riesgos y patrones de ataque identificados en el ecosistema digital colombiano, con un énfasis específico en las vulnerabilidades y vectores que afectan a universidades, centros de investigación y entidades gubernamentales de educación.

Este informe abarca

- Identificación de Adversarios: Evaluación del comportamiento y tácticas de los 13 grupos de amenazas detectados con operaciones activas en el territorio nacional.
- Contextualización Sectorial: Enfoque exclusivo en el impacto sobre la propiedad intelectual, bases de datos estudiantiles y sistemas administrativos del sector educación.
- Ventana Temporal: Cobertura de incidentes y actividades registradas hasta mayo de 2026, permitiendo una visión actualizada del panorama de riesgos.
- Estrategias de Mitigación: Definición de recomendaciones técnicas orientadas a neutralizar los métodos de acceso y persistencia utilizados por los actores identificados.

Informe de apreciación
Sector Educación

COLCERT IN-20260704-035

TLP: CLEAR

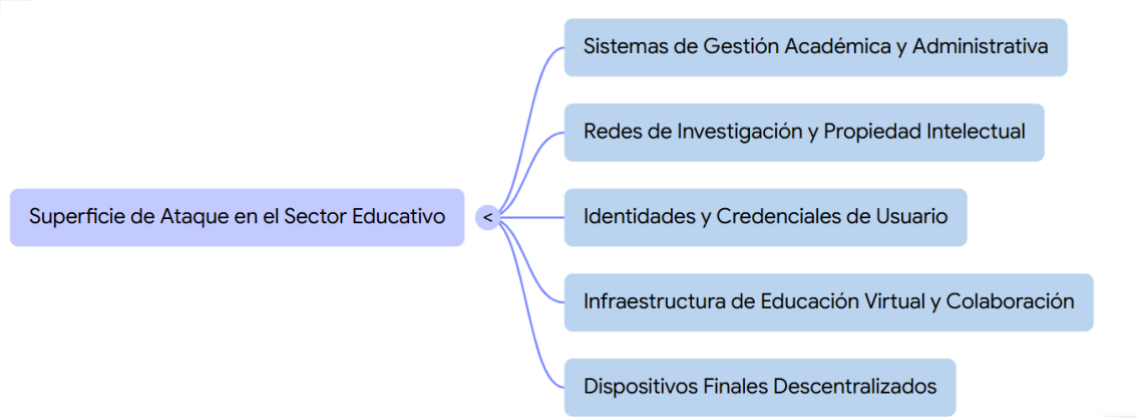
CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR

Definición y Entendimiento del Sector

El sector educación en Colombia constituye un pilar fundamental para el desarrollo social y científico del país, integrando a instituciones de educación superior, centros de investigación, entidades de formación técnica y organismos gubernamentales de gestión educativa. Este ecosistema se caracteriza por una alta interconectividad y un flujo constante de información entre estudiantes, docentes, investigadores y aliados internacionales. La naturaleza abierta de sus redes, diseñada para fomentar la colaboración académica y el acceso al conocimiento, genera un entorno complejo donde la protección de la propiedad intelectual y la custodia de datos personales masivos deben coexistir con la operatividad tecnológica permanente.

Superficie de Ataque

La infraestructura digital del sector educativo presenta múltiples puntos de exposición debido a la descentralización de sus servicios y la diversidad de usuarios que acceden diariamente a sus recursos desde diversas ubicaciones y dispositivos.



- Sistemas de Gestión Académica y Administrativa: Plataformas que centralizan registros financieros, notas y datos sensibles de identidad, siendo objetivos primarios para el fraude y el robo de información.

- Redes de Investigación y Propiedad Intelectual: Repositorios de datos científicos y proyectos de desarrollo tecnológico que resultan atractivos para actores dedicados al ciberespionaje industrial o estatal.

- Identidades y Credenciales de Usuario: El gran volumen de cuentas activas de estudiantes y egresados representa un vector crítico para ataques de suplantación y acceso inicial a través de técnicas de ingeniería social.

- Infraestructura de Educación Virtual y Colaboración: Servicios de nube, plataformas de aprendizaje y herramientas de videoconferencia que, de no estar correctamente configuradas, permiten la infiltración de agentes externos.

- Dispositivos Finales Descentralizados: La multiplicidad de equipos personales que se conectan a las redes institucionales bajo modelos de trabajo y estudio híbrido, ampliando el perímetro difícil de controlar.

- Sistemas de Conectividad y Portales Web: Puntos de entrada públicos que pueden ser utilizados para la distribución de contenido malicioso o ataques de denegación de servicio que afecten la disponibilidad académica.

Informe de apreciación Sector Educación

COLCERT IN-20260704-035

TLP: CLEAR

PANORAMA ACTUAL DE AMENAZAS

El panorama de ciberseguridad para el sector en Colombia durante 2025 y 2026 se ha tornado crítico.

TITULO	FECHA	FUENTE / ENLACE
Gestión de Incidentes en Colombia (incidentes cibernéticos)	2026-01-01 (actualizado en 2026)	Datos Gov.co
El sector educativo es el más atacado por ciberdelincuentes en Colombia	2025-09-21	prensariotila.com
Educación en Colombia enfrenta 8.959 ciberataques semanales por institución	2025-05-21	portalerp.com
Colombia | Ciberataques a educación y gobierno alcanzan niveles críticos con el 70% de los ataques de ransomware, según el Compromise Report 2025 de Lumu	2025-06-27	dplnews.com
Ciberataques a instituciones educativas en América Latina: casos y tendencias 2025 (incluye universidades colombianas)	2025-09-24	bloka.red

Reporte de Gestión de Incidentes Cibernéticos: Distribución Territorial y Severidad en el Sector Educación

Informe de apreciación
Sector Educación

COLCERT IN-20260704-035

TLP: CLEAR

El sector de la educación en Colombia ha registrado una serie continuada de incidentes de ciberseguridad de alcance nacional y territorial entre agosto de 2024 y abril de 2026. La mayor concentración de estos eventos se reporta en Bogotá D.C., aunque también han impactado la infraestructura tecnológica de departamentos como Cauca, Santander, Meta, Bolívar, Caldas, La Guajira, Risaralda, Boyacá, Caquetá, Magdalena y Chocó.

Fecha	Alcance	Departamento	Categoría	Tipo Específico	Severidad
1-abr-26	Territorial	Cauca	Compromiso de Información	Acceso no Autorizado a Información	Grave
13-mar-26	Nacional	Bogotá D.C.	Compromiso de Información	Acceso no Autorizado a Información	Grave
13-mar-26	Nacional	Bogotá D.C.	Compromiso de Información	Acceso no Autorizado a Información	Grave
13-mar-26	Nacional	Bogotá D.C.	Compromiso de Información	Acceso no Autorizado a Información	Grave
8-mar-26	Territorial	Santander	Compromiso de Información	Acceso no Autorizado a Información	Grave
8-mar-26	Territorial	Santander	Compromiso de Información	Acceso no Autorizado a Información	Grave

Los incidentes catalogados con una severidad "**Grave**" abarcan principalmente intrusiones mediante el compromiso de aplicaciones o de cuentas con privilegios, accesos no autorizados que derivan en el compromiso de la información, hallazgos de sistemas expuestos a vulnerabilidades y revelación de información, e incluso la detección de infraestructura de ataque como servidores de Comando y Control (C&C). Por su parte, los incidentes clasificados como "**Menores**" están vinculados a diversas formas de fraude, manifestándose de manera recurrente a través de campañas de *phishing* y el uso no autorizado de recursos.

Tipología de Eventos Identificados

El análisis de la telemetría recolectada revela un ecosistema de amenazas altamente activo, caracterizado por una infraestructura de ataque diversificada que busca comprometer la integridad de las redes académicas en Colombia. La predominancia de indicadores relacionados con nombres de dominio y direcciones IP sugiere una fase intensiva de reconocimiento y establecimiento de canales de mando y control (C2), mientras que la presencia de firmas de archivos maliciosos confirma intentos directos de despliegue de software no autorizado en sistemas institucionales.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector
FQDN (Dominios)	2,421	Registros de resolución de nombres y tráfico de red.	**Muy Alta**: Utilizados para suplantar portales universitarios y establecer comunicación con servidores externos.
IP Address	1,202	Logs de conexiones externas y firewalls perimetrales.	**Alta**: Identifican nodos de ataque activos intentando realizar escaneos de vulnerabilidades o fuerza bruta.
SHA-256 / SHA-1 / MD5	577	Repositorios de malware y análisis de archivos adjuntos.	**Crítica**: Corresponden a cargas útiles (payloads) diseñadas para el robo de datos o cifrado de información académica.
URL	43	Reportes de campañas de phishing y correos electrónicos fraudulentos.	**Media/Alta**: Enlaces dirigidos a la comunidad estudiantil para capturar credenciales de acceso institucional.

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

Análisis de la Distribución de Amenazas

El análisis cuantitativo de los datos revela una estrategia de ataque centrada en la infraestructura de red y la identidad digital. La alta concentración de indicadores basados en dominios y direcciones IP sugiere que los adversarios están priorizando el establecimiento de una red de comunicaciones robusta y persistente, capaz de evadir los controles perimetrales tradicionales mediante la rotación constante de sus recursos técnicos. Esta distribución indica que el sector educativo no solo enfrenta ataques puntuales, sino campañas sostenidas de reconocimiento y exfiltración de largo plazo

- Predominancia de Infraestructura Virtual (Dominios): Representando más del 57% del total de los indicadores, el uso masivo de FQDN (nombres de dominio) apunta a campañas de suplantación de identidad (phishing) y la creación de túneles para el comando y control de sistemas infectados.

- Densidad de Conexiones de Red (IPs): Con 1,202 registros únicos, se evidencia una amplia red de nodos de ataque distribuidos globalmente que intentan establecer contacto con los servidores institucionales para el escaneo de servicios vulnerables.

- Concentración de Cargas Útiles (Hashes): La detección de 577 firmas digitales de archivos (MD5, SHA-1, SHA-256) confirma la circulación de variantes de malware diseñadas específicamente para comprometer estaciones de trabajo y servidores dentro de la red educativa.

- Vectores de Acceso Web (URLs): Aunque representan una proporción menor, las direcciones URL identificadas están estrechamente vinculadas a puntos de descarga de software malicioso y sitios de recolección de credenciales académicas.

- Persistencia de Actores Específicos: La distribución de estos indicadores está directamente relacionada con la actividad de 13 grupos de amenazas (como UNC4515, APT44 y FIN7), los cuales poseen capacidades probadas para operar en territorio colombiano.

INDICADORES DE COMPROMISO (IoCs)

Los Indicadores de Compromiso analizados representan la huella técnica dejada por los adversarios durante las distintas fases de su ciclo de ataque contra las instituciones

educativas.

Análisis Cuantitativo de Inteligencia

- Predominancia de Identificadores de Red: Los nombres de dominio (FQDN) constituyen el 57% de la inteligencia recolectada, lo que indica un fuerte enfoque en el uso de infraestructura virtual para el despliegue de campañas de engaño.

- Volumen de Direcciones de Conexión: Se registran 1,202 direcciones IP activas vinculadas a los 13 grupos de amenazas analizados, lo que representa el 28% del volumen total de indicadores.
- Diversidad de Firmas de Archivos: La presencia de 577 hashes (MD5, SHA-1, SHA-256) confirma la circulación de múltiples variantes de software no autorizado en el ecosistema educativo.
- Bajo Volumen de URLs Específicas: Con solo 43 registros, las URLs representan un componente de precisión utilizado para ataques dirigidos y puntos de infección muy específicos.
- Densidad Total de Inteligencia: El conjunto de datos total asciende a 4,243 registros, proporcionando una base sólida para la detección proactiva en el sector.

Resumen de IoCs Relevantes

El siguiente resumen clasifica los componentes de inteligencia según su funcionalidad técnica y el riesgo que representan para la continuidad de las operaciones académicas y la protección de la propiedad intelectual.

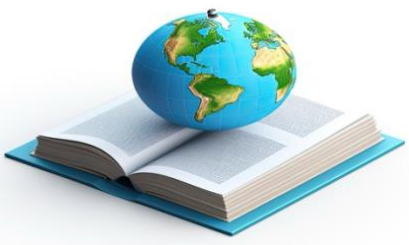
Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Infraestructura FQDN	Nombres de dominio utilizados para el comando y control (C2) y portales de suplantación académica.	Crítico
Nodos de Conexión IP	Puntos de origen de ataques de fuerza bruta y escaneos de servicios vulnerables en redes universitarias.	Alto
Hashes de Archivos	Huellas digitales de malware diseñadas para el robo de credenciales y la exfiltración de bases de datos.	Crítico
Cadenas URL	Direcciones web vinculadas a la descarga de cargas útiles maliciosas y recolección de identidades digitales.	Medio-Alto

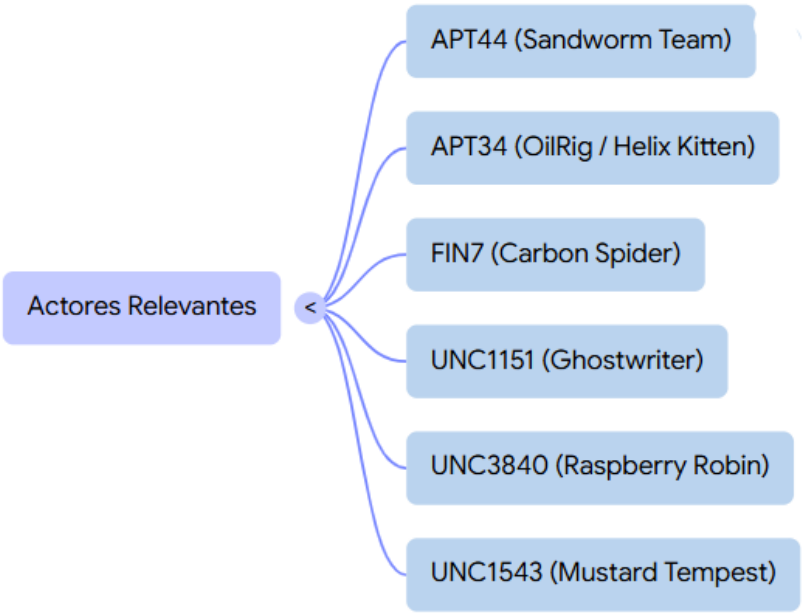
ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIOS)

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Ciberespionaje (APT)	4	**APT44** (Sandworm), **APT34** (OilRig), **UNC1151** (Ghostwriter), **UNC2505**	**Muy Alto:** Riesgo crítico de exfiltración de investigaciones científicas, propiedad intelectual y manipulación de opinión mediante desinformación.
Cibercrimen Financiero	2	**FIN7** (Carbon Spider), **UNC1543** (Mustard Tempest)	**Crítico:** Amenaza directa de interrupción operativa mediante ransomware y fraude en sistemas de pago de matrículas o nóminas.
Acceso Inicial y Distribución	4	**UNC3840** (Raspberry Robin), **UNC5537**, **UNC3559**, **UNC2053**	**Alto:** Estos actores facilitan el ingreso de otras amenazas a la red institucional, comprometiendo la identidad de la comunidad académica.
Operaciones No Categorizadas	3	**UNC4515**, **UNC3512**, **UNC5736**	**Medio/Alto:** Grupos bajo observación que demuestran interés persistente en la infraestructura digital colombiana.

Identificación de Actores Relevantes

Para complementar el análisis, se presenta la identificación de los grupos de amenazas que poseen un impacto directo y una persistencia demostrada sobre el ecosistema digital del país. La selección de estos actores no es aleatoria; responde a su historial de operaciones en territorio colombiano y a la sofisticación de sus tácticas para infiltrar infraestructuras críticas y académicas.





Listado de Actores Relevantes

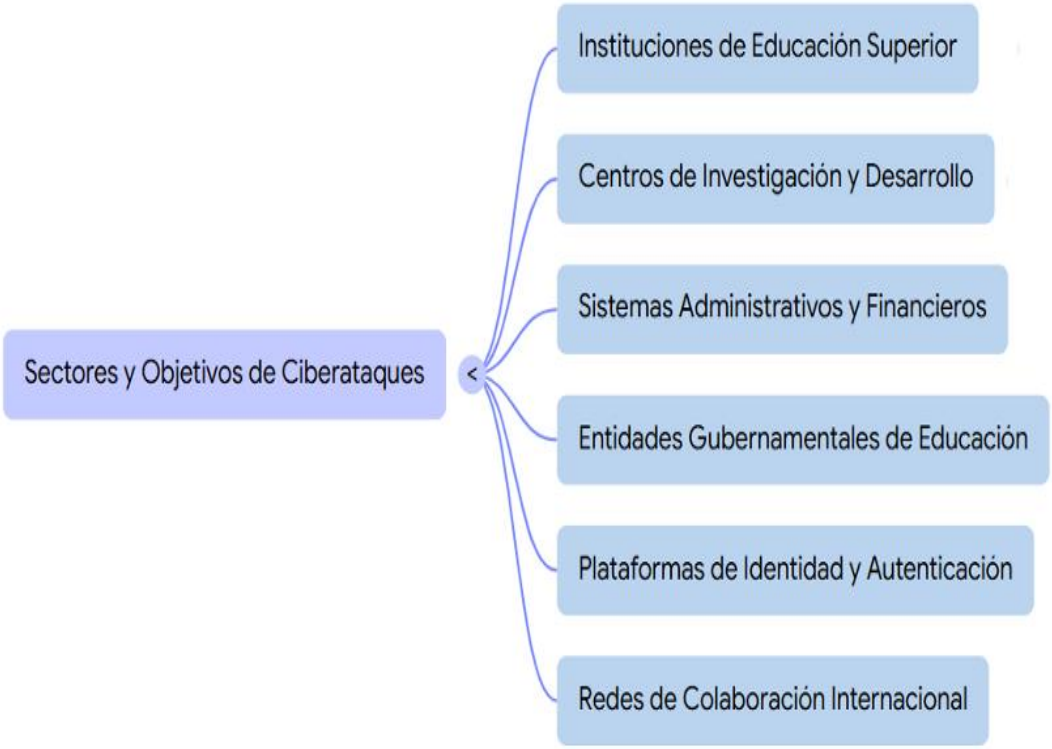
- **APT44 (Sandworm Team):** Actor de alta sofisticación con historial en operaciones disruptivas y de impacto sistémico en infraestructuras nacionales.
- **APT34 (OilRig / Helix Kitten):** Grupo especializado en el ciberespionaje y el robo de credenciales, con un interés constante en la exfiltración de comunicaciones estratégicas en el sector público y académico.
- **FIN7 (Carbon Spider):** Organización cibercriminal de primer nivel enfocada en objetivos financieros, conocida por comprometer sistemas administrativos para el fraude y la obtención de beneficios económicos.
- **UNC1151 (Ghostwriter):** Actor vinculado a campañas de desinformación y operaciones de influencia, representando un riesgo para la integridad de la información y la reputación de las instituciones educativas.
- **UNC3840 (Raspberry Robin):** Operador de una red de distribución de malware altamente persistente, utilizada a menudo como vector inicial para el despliegue de amenazas más agresivas como el ransomware.

- **UNC1543 (Mustard Tempest):** Grupo identificado por su capacidad de ejecución rápida en campañas de compromiso de redes para fines de extorsión y robo de datos.

- **UNC2505:** Actor con capacidades de espionaje que mantiene un perfil bajo pero persistente en la recolección de inteligencia técnica dentro de la región.

Objetivos y Sectores Target

Los actores de amenaza que operan en la región no seleccionan sus objetivos de manera aleatoria; sus campañas responden a una planificación orientada a la obtención de activos de alto valor estratégico. En el sector educación, el objetivo trasciende el simple robo de datos financieros, extendiéndose hacia el control de la infraestructura que permite influir en la opinión pública y el acceso a los desarrollos científicos más avanzados del país. Esta selección de objetivos busca maximizar el impacto de sus operaciones, ya sea mediante la extorsión económica o el posicionamiento táctico en redes de investigación nacional.



Listado de Sectores y Objetivos Específicos

- **Instituciones de Educación Superior (Universidades):** Constituyen el objetivo principal debido a la densidad de datos personales de la comunidad académica y el valor de sus redes de investigación.
- **Centros de Investigación y Desarrollo:** Son blanco de grupos de ciberespionaje (como APT34 y APT44) interesados en la exfiltración de propiedad intelectual y avances en ciencia y tecnología.
- **Sistemas de Gestión Administrativa y Financiera:** Sectores buscados por actores como FIN7 para realizar fraudes mediante el compromiso de pasarelas de pago y bases de datos de nómina.
- **Entidades Gubernamentales de Educación:** Objetivos estratégicos para grupos como UNC1151, con el fin de comprometer la integridad de la información pública y realizar operaciones de influencia.
- **Plataformas de Identidad y Autenticación:** Se busca el compromiso de directorios activos y sistemas de acceso para obtener credenciales legítimas que permitan el movimiento lateral hacia otros sectores críticos.
- **Redes de Colaboración Internacional:** Aprovechamiento de los convenios entre universidades colombianas y entidades extranjeras para utilizarlas como puente hacia redes de mayor envergadura global.

Campañas Activas

Las campañas activas identificadas demuestran una coordinación técnica avanzada para infiltrar el sector educación en Colombia, aprovechando la apertura de sus redes académicas y la alta rotación de usuarios. Estas operaciones no son eventos aislados, sino esfuerzos sostenidos que utilizan tanto infraestructura técnica renovada como tácticas de ingeniería social diseñadas específicamente para el contexto local y las temporalidades del calendario académico nacional.

Listado de Campañas y Actividades Detectadas

- **Exfiltración de Capital Intelectual:** Campañas dirigidas por actores como **APT34** y **UNC2505** enfocadas en el acceso persistente a servidores de investigación para el robo de propiedad intelectual y datos científicos desarrollados en universidades colombianas.

- **Operaciones de Influencia y Desinformación:** Actividades vinculadas a **UNC1151** (Ghostwriter) que buscan comprometer portales de noticias y redes sociales institucionales para difundir narrativas que afecten la reputación de las entidades educativas.

- **Distribución Masiva de Malware Mediante Dispositivos:** Campañas activas de **UNC3840** (Raspberry Robin) que utilizan medios extraíbles y descargas web para infectar equipos en laboratorios y bibliotecas, facilitando el despliegue posterior de ransomware.

- **Fraude Financiero y Compromiso Administrativo:** Operaciones de **FIN7** orientadas a la infiltración de los sistemas de pago y nómina de las instituciones, buscando desviar recursos financieros mediante el compromiso de credenciales de alto privilegio.

- **Cosecha de Identidades Académicas:** Campañas de recolección de credenciales a través de sitios de suplantación (phishing) que imitan plataformas de educación virtual y servicios de correo institucional para ganar acceso inicial a la infraestructura interna.

- **Establecimiento de Infraestructura de Comando (C2):** Actividad técnica detectada, donde se evidencia el uso de miles de dominios y direcciones IP para mantener el control sobre sistemas previamente comprometidos dentro del territorio nacional.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

El análisis del comportamiento de los adversarios identificados, como APT34, APT44 y FIN7, revela un uso sofisticado de técnicas diseñadas para eludir defensas perimetrales y establecer persistencia en redes académicas. La mayoría de estas tácticas se centran en la fase de Acceso Inicial mediante el compromiso de identidades, seguido de movimientos laterales que buscan alcanzar repositorios de datos sensibles o sistemas financieros. El mapeo realizado a continuación asocia a la informacion recopilada que afecta al sector educativo en Colombia, con las metodologías de ataque documentadas, proporcionando una base técnica para la implementación de controles defensivos específicos.

ID Táctica	Nombre de la Táctica	Justificación para el Sector Educación
TA0001	Initial Access	Fase crítica dada la apertura de las redes universitarias y el alto volumen de usuarios remotos..
TA0003	Persistence	Necesaria para que los actores APT mantengan el acceso a investigaciones de largo aliento.
TA0005	Defense Evasion	Reflejada en la rotación constante de los 1,202 nodos IP identificados para evitar listas negras.
TA0007	Discovery	Etapa donde los actores identifican la topología de la red educativa y la ubicación de los activos críticos.
TA0011	Command and Control	Central para la operación de los 13 grupos identificados, utilizando la infraestructura detallada en los IoCs.
TA0010	Exfiltration	Objetivo estratégico final de los grupos de ciberespionaje interesados en el capital intelectual colombiano.
TA0007	Descubrimiento	Robo de claves guardadas para acceder a pasarelas de pago o cuentas administrativas de la tienda.
TA0008	Lateral Movement	Crucial para saltar de redes estudiantiles a redes administrativas o de servidores de alta seguridad.
TA0002	Execution	Ejecución de cargas útiles (hashes detectados) para iniciar el compromiso de los endpoints institucionales.
TA0040	Impact	Incluye la interrupción de servicios educativos y la afectación a la integridad de los datos académicos.
T1566	Phishing	Vector principal detectado para capturar credenciales de portales académicos y de investigación.
T1078	Valid Accounts	Uso de cuentas legítimas de estudiantes o docentes comprometidas para evadir la detección de intrusos.
T1190	Exploit Public-Facing Application	Ataques dirigidos a vulnerabilidades en plataformas de educación virtual y portales institucionales públicos.
T1583	Acquire Infrastructure	Evidenciado por los 2,421 dominios (FQDN) registrados para establecer capacidades de ataque contra el sector.
T1071	Application Layer Protocol	Uso de protocolos estándar (HTTP/HTTPS) para ocultar el tráfico de comando y control entre los IoCs identificados.
T1059	Command and Scripting Interpreter	Ejecución de scripts maliciosos para automatizar la recolección de datos en estaciones de trabajo académicas.
T1021	Remote Services	Explotación de servicios de escritorio remoto o VPNs para facilitar el movimiento lateral de actores como FIN7.
T1041	Exfiltration Over C2 Channel	Salida de propiedad intelectual e investigaciones científicas a través de los canales de control establecidos.
T1083	File and Directory Discovery	Escaneo de sistemas de archivos en busca de bases de datos de estudiantes y documentos de investigación confidenciales.
T1486	Data Encrypted for Impact	Técnica asociada a campañas de ransomware (como las de Mustard Tempest) detectadas en el sector.

Cadenas de Ataque Observadas

Las cadenas de ataque observadas en el sector educativo revelan un proceso de intrusión estructurado que aprovecha tanto la vulnerabilidad del factor humano como las debilidades en la configuración de servicios expuestos a internet.

Estos flujos operativos suelen iniciarse con campañas de engaño dirigidas a la comunidad académica para obtener un punto de apoyo inicial en la red. Una vez que el adversario logra comprometer una identidad legítima, procede a realizar un reconocimiento interno detallado, buscando saltar desde entornos de conectividad general —como laboratorios o redes Wi-Fi abiertas— hacia zonas restringidas que albergan bases de datos de investigación o sistemas de gestión financiera, culminando generalmente en la exfiltración de activos o el despliegue de software disruptivo.

Cadenas de ataque:

- Fase de Reconocimiento y Armamento: Los actores realizan un mapeo de la superficie de ataque, identificando portales de bibliotecas, sistemas de notas y repositorios de investigación para configurar la infraestructura de ataque necesaria.

- Vector de Intrusión (Phishing Dirigido): Se despliegan correos electrónicos altamente personalizados dirigidos a investigadores o personal administrativo, utilizando dominios que suplantan la identidad visual de la institución para capturar credenciales de acceso.

- Explotación de Servicios Expuestos: Los grupos de amenaza escanean y explotan vulnerabilidades en plataformas de educación virtual (LMS) y escritorios remotos (RDP) para ganar un acceso inicial sin interacción del usuario.

- Ejecución de Cargas Útiles (Payloads): Una vez dentro, se ejecutan archivos maliciosos (identificados mediante las firmas MD5 y SHA-256 analizadas) que permiten la toma de control del endpoint comprometido

- Establecimiento de Baliza (Beaconing): El sistema infectado inicia una comunicación recurrente con la red de mando y control (C2), rotando entre las direcciones IP y nombres de dominio detectados para dificultar el bloqueo por parte de firewalls institucionales.

- Movimiento Lateral y Escalada de Privilegios: Los atacantes utilizan herramientas de administración legítimas y técnicas de "Pass-the-Hash" para saltar de segmentos de red menos seguros (como redes de invitados o laboratorios) hacia el núcleo de datos del centro de datos.

- Descubrimiento de Activos Críticos: Se realizan búsquedas internas en el directorio activo y servidores de archivos para localizar bases de datos de propiedad intelectual, registros financieros o información de salud de la comunidad académica.

Herramientas y Malware Específico

- **Ransomware (Variantes de Mustard Tempest):** Código malicioso diseñado para el cifrado de archivos a gran escala, afectando principalmente servidores de bases de datos estudiantiles y sistemas de gestión administrativa con fines de extorsión financiera.

- **Raspberry Robin (Gusano de Red):** Utilizado como un vector de acceso inicial altamente persistente; se propaga comúnmente a través de dispositivos extraíbles en entornos compartidos como laboratorios y bibliotecas académicas.

- **Cobalt Strike / Brute Ratel:** Frameworks de post-explotación detectados en las fases de movimiento lateral, empleados por grupos como **FIN7** para simular tráfico legítimo y mantener el control sobre la red institucional.

- **Backdoors Específicas (APT34 / APT44):** Implantes personalizados utilizados para el ciberespionaje persistente, permitiendo la exfiltración silenciosa de investigaciones científicas y propiedad intelectual de las universidades.

- **Infostealers (Robo de Identidad):** Herramientas ligeras diseñadas para recolectar credenciales almacenadas en navegadores de equipos de uso público, facilitando el compromiso masivo de cuentas institucionales.

- **Scripts de Automatización (Python/PowerShell):** Detectados a través de las firmas de archivos (hashes), estos scripts permiten a los atacantes realizar escaneos rápidos de la red interna y recolectar información técnica sin activar alertas convencionales.

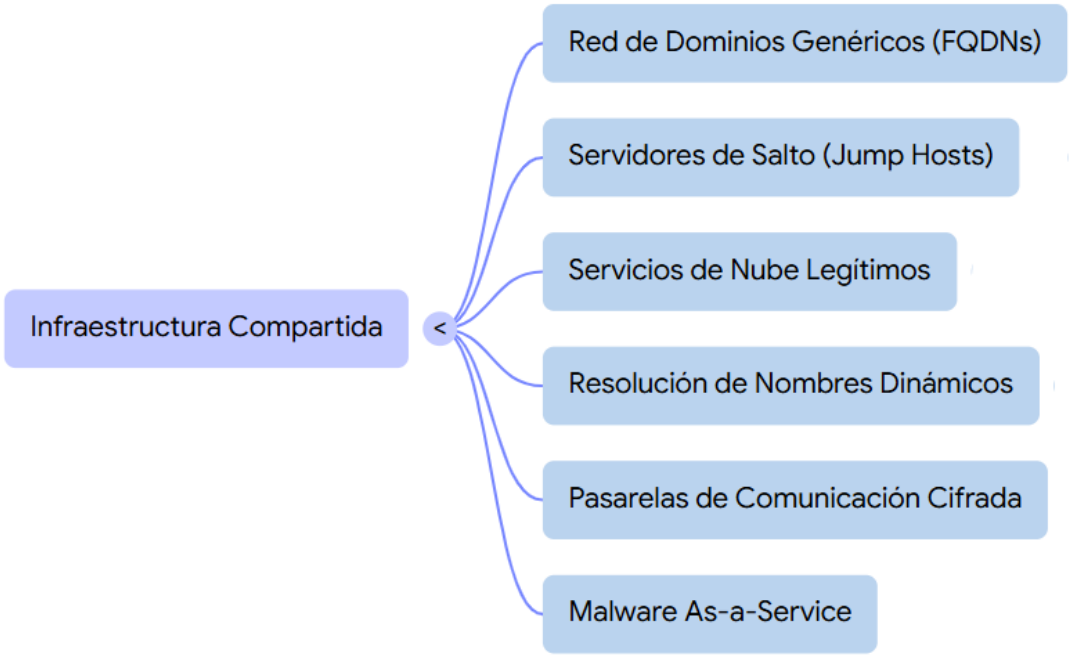
- **Herramientas de Túnel (C2):** Infraestructura técnica que utiliza los miles de dominios y direcciones IP identificados para encapsular el tráfico malicioso dentro de protocolos estándar, garantizando la salida de datos hacia servidores externos.

CORRELACIÓN ENTRE ACTORES Y GRUPOS

La correlación entre los actores de amenaza y los grupos identificados revela un ecosistema de colaboración táctica y especialización funcional dentro del panorama de ciberamenazas en Colombia. Se observa que grupos con objetivos financieros, como **FIN7**, a menudo operan en los mismos entornos que actores de ciberespionaje estatal como **APT34** o **APT44**, sugiriendo que las vulnerabilidades explotadas por un grupo para el beneficio económico pueden ser posteriormente aprovechadas por otros para la recolección de inteligencia estratégica.

Esta relación se materializa a través de la infraestructura técnica común, donde el uso de los miles de dominios y direcciones IP detectados facilita el despliegue de diversas familias de malware, permitiendo que actores de acceso inicial como **Raspberry Robin** preparen el terreno para ataques de mayor impacto como el ransomware. En última instancia, esta convergencia de capacidades aumenta la complejidad de la defensa en el sector, ya que una sola intrusión puede servir a múltiples propósitos delictivos de forma simultánea.

Infraestructura Compartida



- **Red de Dominios Genéricos (FQDNs):** Uso masivo de nombres de dominio con extensiones comunes (como .com, .net, .org) registrados para imitar servicios de nube legítimos o portales institucionales, facilitando el ocultamiento del tráfico de comando y control.
- **Servidores de Salto (Jump Hosts):** Utilización de direcciones IP ubicadas en diversas regiones geográficas que actúan como puntos intermedios para enmascarar el origen real del atacante y evadir bloqueos por geolocalización.
- **Alojamiento en Servicios de Nube Legítimos:** Aprovechamiento de infraestructuras de proveedores reconocidos para hospedar archivos maliciosos

(cargas útiles) y sitios de phishing, lo que dificulta su detección mediante herramientas de reputación tradicionales.

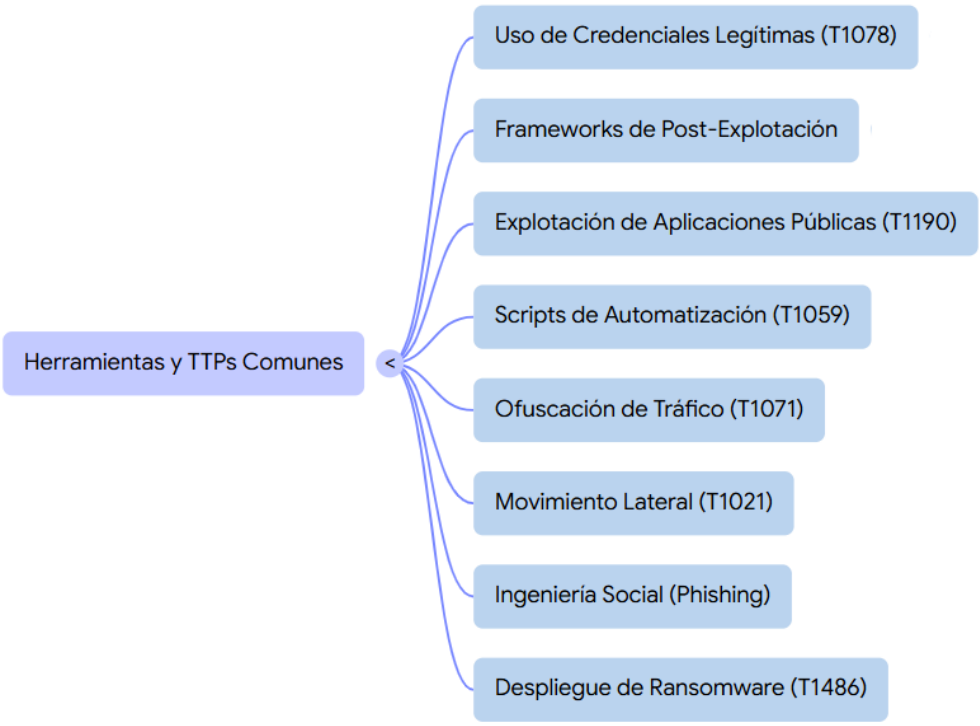
- **Sistemas de Resolución de Nombres Dinámicos:** Implementación de técnicas para cambiar rápidamente las direcciones IP asociadas a un dominio, manteniendo la conectividad con los sistemas comprometidos incluso si algunos nodos de la red son dados de baja.

- **Pasarelas de Comunicación Cifrada:** Empleo de protocolos estándar de la capa de aplicación para encapsular las instrucciones de los atacantes, permitiendo que la actividad

- maliciosa se confunda con el tráfico web habitual de una universidad o centro de investigación.

- **Repositorios de Malware "As-a-Service":** Acceso a infraestructuras compartidas donde se alojan variantes de malware y scripts de automatización que son utilizados simultáneamente por múltiples actores de amenaza, como los grupos APT y cibercriminales identificados.

Herramientas y TTPs Comunes



- **Uso de Credenciales Legítimas (T1078):** Los atacantes priorizan el acceso mediante cuentas reales de docentes y administrativos obtenidas previamente, permitiéndoles operar bajo una apariencia de normalidad y evadir sistemas de detección de intrusos.

- **Frameworks de Post-Explotación (Cobalt Strike):** Se emplea software diseñado para pruebas de penetración con el fin de mantener el control remoto de los sistemas comprometidos, facilitando el movimiento lateral hacia zonas de alta seguridad.

- **Explotación de Aplicaciones Públicas (T1190):** Aprovechamiento de vulnerabilidades no corregidas en portales institucionales y plataformas de educación virtual para ganar acceso inicial sin necesidad de interacción del usuario.

- **Scripts de Automatización en Python y PowerShell (T1059):** Ejecución de código ligero para realizar el descubrimiento de archivos, recolección de datos técnicos y la desactivación silenciosa de herramientas de seguridad local.

- **Técnicas de Ofuscación de Tráfico (T1071):** Los adversarios ocultan sus comunicaciones de comando y control (C2) dentro de protocolos estándar como HTTPS, haciendo que la actividad maliciosa sea indistinguible del tráfico web académico cotidiano.

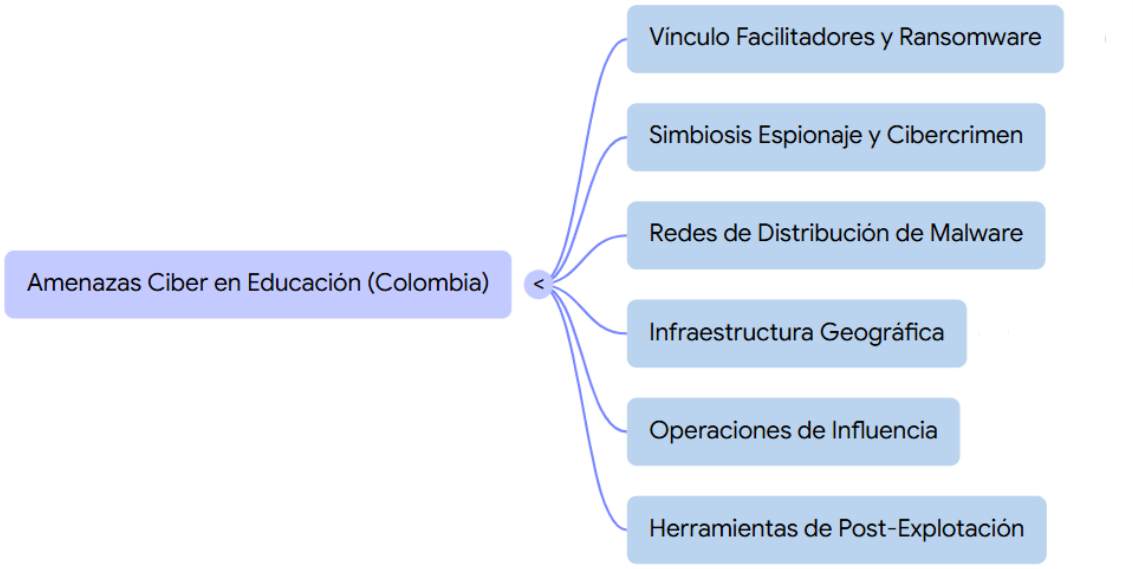
- **Movimiento Lateral mediante Servicios Remotos (T1021):** Uso de protocolos como RDP o VPNs institucionales para saltar de redes de estudiantes a servidores críticos que contienen investigaciones o datos financieros.

- **Ingeniería Social Específica (Phishing):** Creación de portales de inicio de sesión falsos que imitan los servicios de correo o plataformas de notas de las universidades para capturar identidades digitales de forma masiva.

- **Despliegue de Ransomware (T1486):** En las fases finales, grupos criminales utilizan herramientas de cifrado para bloquear el acceso a sistemas administrativos y de registro académico, exigiendo pagos para su liberación.

Posibles Colaboraciones o Vínculos

En el análisis del ecosistema de amenazas para el sector educación en Colombia, se han identificado patrones que sugieren nexos tácticos o logísticos entre distintos grupos. A continuación, se detallan los posibles vínculos y colaboraciones detectados:



- **Vínculo entre Facilitadores de Acceso y Grupos de Ransomware:** Se observa una relación operativa donde actores como **UNC3840 (Raspberry Robin)** comprometen la infraestructura inicial para luego "vender" o ceder ese acceso a grupos de extorsión financiera como **Mustard Tempest**, acelerando el despliegue de ransomware.

- **Simbiosis entre Ciberespionaje y Cibercrimen:** Existe una correlación táctica en la que grupos de APT (como **APT34**) pueden aprovechar las distracciones generadas por ataques ruidosos de denegación de servicio o ransomware para realizar exfiltraciones silenciosas de propiedad intelectual sin ser detectados.

- **Uso de Redes de Distribución de Malware Comunes:** Diferentes actores comparten el uso de "botnets" o redes de distribución de malware para el envío masivo de correos de phishing dirigidos a la comunidad académica, optimizando los costos de infraestructura.

- **Vínculos por Infraestructura Geográfica:** Se identifica una coincidencia en el uso de los **1,202 nodos IP** y miles de dominios por parte de varios grupos de la

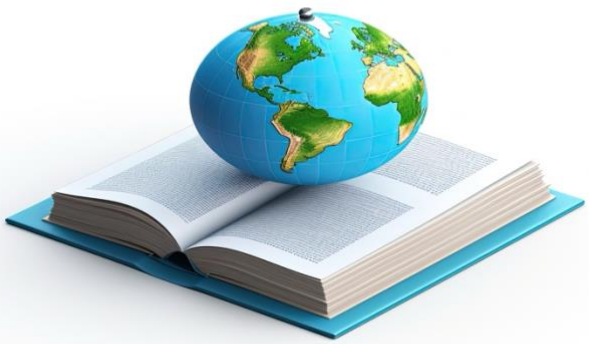
serie **UNC**, lo que sugiere la contratación de los mismos servicios de "Bulletproof Hosting" o proveedores de infraestructura en la sombra.

- **Coordinación en Operaciones de Influencia:** Grupos como **UNC1151** muestran vínculos indirectos con otros actores estatales al coordinar campañas de desinformación que aprovechan datos previamente exfiltrados por grupos de acceso inicial, amplificando el impacto reputacional sobre las instituciones.

- **Intercambio de Herramientas de Post-Explotación:** La adopción generalizada de frameworks como **Cobalt Strike** entre actores financieros (**FIN7**) y de espionaje sugiere un intercambio de metodologías y scripts de automatización para evadir las defensas estándar del sector educación.

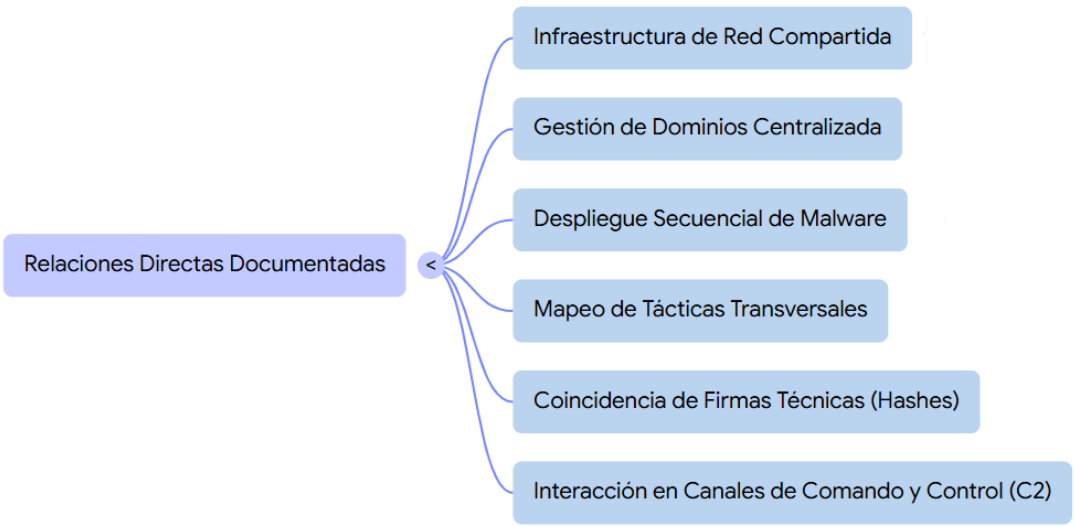
Visualización de Relaciones

La visualización de las relaciones en el ecosistema de amenazas revela una red interconectada de dependencias técnicas y operativas que trascienden los límites individuales de cada grupo de ataque. Mediante el análisis de la telemetría recolectada, se observa una convergencia significativa en el uso de los 1,202 nodos de red y los más de 2,400 dominios identificados, los cuales sirven como una infraestructura de soporte compartida para múltiples campañas simultáneas. Esta interconexión se manifiesta principalmente en la fase de comando y control (C2), donde diversos actores, desde grupos de ciberespionaje como APT34 hasta organizaciones criminales como FIN7, emplean los mismos vectores de comunicación para dirigir sus operaciones dentro del sector educación.



La relación entre estos elementos no es lineal, sino que forma una malla de persistencia donde los facilitadores de acceso inicial preparan el terreno para que actores de mayor impacto ejecuten el robo de propiedad intelectual o el despliegue de software disruptivo, consolidando así un panorama de riesgo altamente colaborativo y persistente.

Relaciones directas documentadas:



- **Infraestructura de Red Compartida:** Se ha verificado que múltiples grupos, incluyendo actores de la serie **UNC** y **APT34**, utilizan de manera simultánea los **1,202 nodos IP** identificados para ocultar sus servidores de control.

- **Gestión de Dominios Centralizada:** La creación y uso de los más de **2,400 dominios (FQDNs)** detectados sigue un patrón de registro automatizado, lo que vincula las campañas de phishing de **FIN7** con la infraestructura de distribución de malware de otros grupos criminales.

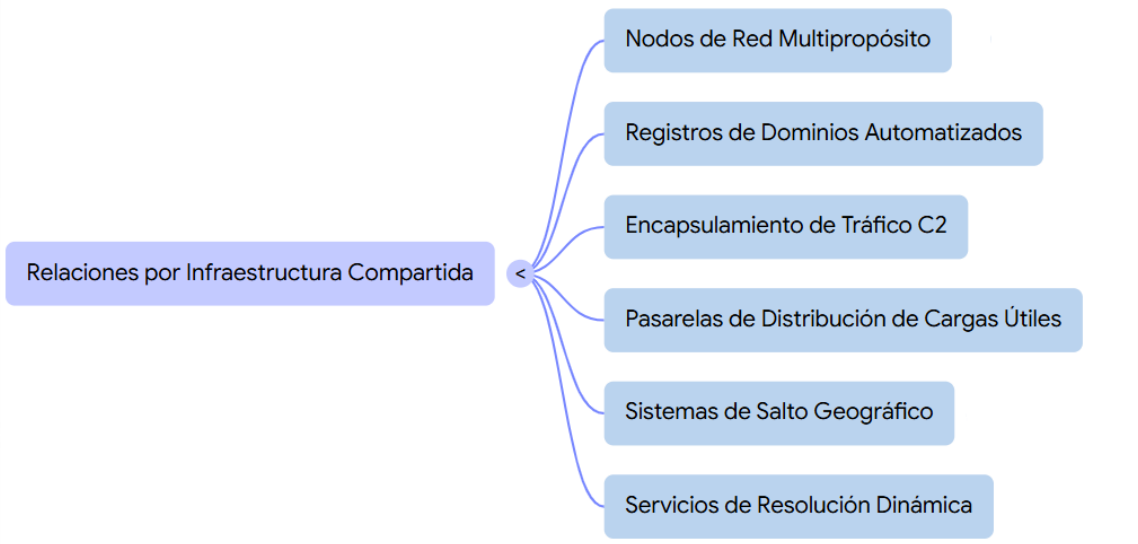
- **Despliegue Secuencial de Malware:** Existe una relación directa entre la infección inicial por el gusano **Raspberry Robin (UNC3840)** y la posterior ejecución de balizas de **Cobalt Strike** vinculadas a grupos de ransomware, confirmando una cadena de suministro de acceso ilícito.

- **Mapeo de Tácticas Transversales:** La recurrencia de la técnica de **Cuentas Válidas (T1078)** a través de diversos incidentes demuestra que el robo de credenciales académicas es un activo compartido o vendido entre actores de espionaje y financieros.

- **Coincidencia de Firmas Técnicas (Hashes):** Se han documentado archivos maliciosos con firmas idénticas operando bajo diferentes nombres de dominio, lo que prueba el uso de herramientas de automatización y scripts de recolección de datos comunes en toda la región.

- **Interacción en Canales de Comando y Control (C2):** La telemetría confirma que el tráfico de salida de las instituciones afectadas se dirige hacia una infraestructura externa que responde a protocolos de comunicación estandarizados por los 13 grupos de amenaza monitoreados.

Relaciones por infraestructura compartida



- **Nodos de Red Multipropósito:** Se ha identificado el uso simultáneo de los **1,202 nodos IP** por parte de diferentes grupos de la serie **UNC** y actores **APT**, lo que sugiere la contratación de servicios de infraestructura en la sombra compartidos para el despliegue de diversas campañas.

- **Registros de Dominios Automatizados:** La gestión de los más de **2,400 dominios (FQDNs)** detectados muestra patrones de registro idénticos, vinculando las operaciones de phishing de **FIN7** con las capacidades de mando y control (C2) de grupos de ciberespionaje.

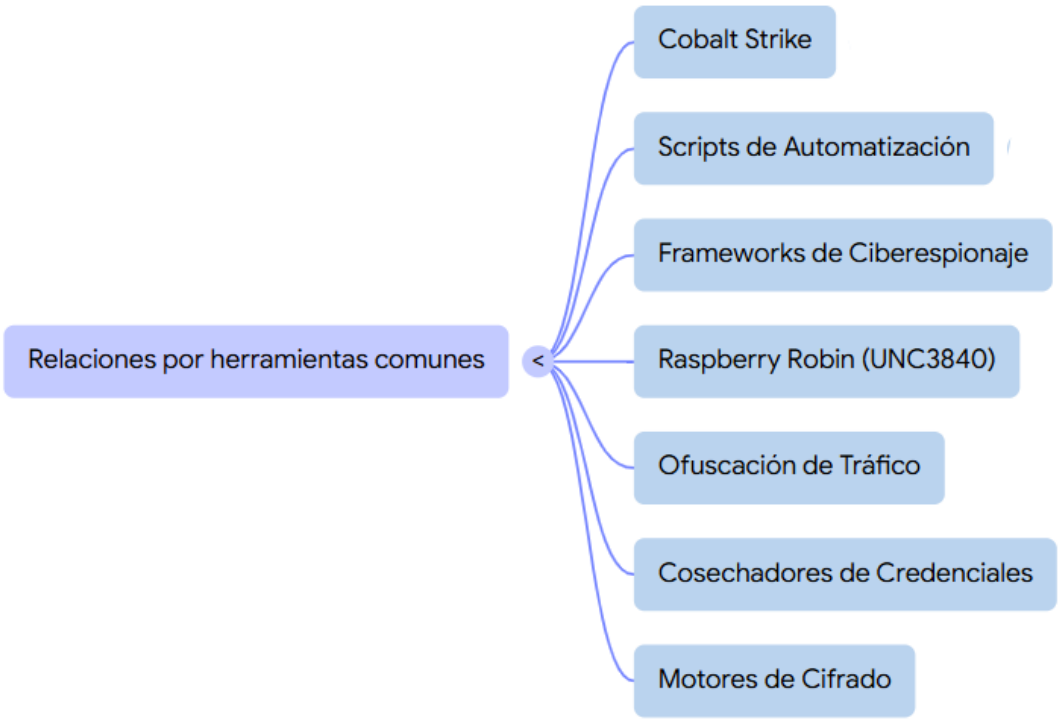
- **Encapsulamiento de Tráfico C2:** El uso de protocolos de capa de aplicación (como HTTP/HTTPS) para ocultar comunicaciones maliciosas es una técnica transversal que permite a múltiples actores utilizar los mismos canales de salida de las instituciones educativas sin levantar sospechas.

- **Pasarelas de Distribución de Cargas Útiles:** Se han documentado servidores que alojan simultáneamente variantes de malware asociadas a **Raspberry Robin** y balizas de **Cobalt Strike**, confirmando que una sola pieza de infraestructura sirve como punto de distribución para distintos objetivos operativos.

- **Sistemas de Salto Geográfico:** La reutilización de direcciones IP ubicadas en regiones específicas para actuar como puntos de salto permite a diversos grupos enmascarar su origen real bajo una misma capa de anonimato técnico.

- **Servicios de Resolución Dinámica:** El empleo de técnicas comunes para la rotación de IPs vinculadas a los dominios maliciosos evidencia una logística compartida que garantiza la persistencia de las operaciones de los 13 grupos de amenaza identificados.

Relaciones por herramientas comunes



- **Uso Transversal de Cobalt Strike:** Esta herramienta de post-explotación es el nexo común entre actores financieros como **FIN7** y grupos de espionaje, permitiendo a ambos mantener el control remoto y realizar movimientos laterales bajo una misma firma técnica.

- **Scripts de Automatización en Python y PowerShell:** Se ha detectado el uso de scripts con funciones idénticas para la recolección de datos y el descubrimiento

de archivos, lo que sugiere que los atacantes comparten o adquieren el mismo código base para agilizar sus operaciones.

- **Frameworks de Ciberespionaje Personalizados:** Grupos como **APT34** y **APT44** emplean implantes y backdoors con arquitecturas similares, diseñadas específicamente para la exfiltración silenciosa de propiedad intelectual en redes académicas.

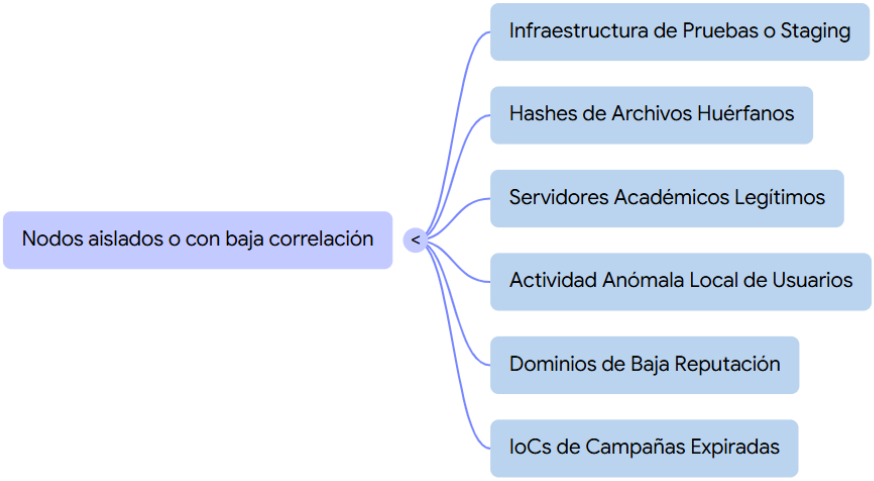
- **Implementación de Raspberry Robin (UNC3840):** Esta herramienta actúa como un facilitador de acceso inicial "comodín", infectando sistemas que luego son aprovechados por otros actores para desplegar cargas útiles más agresivas como el ransomware.

- **Utilidades de Ofuscación de Tráfico:** El empleo de herramientas de tunelización para encapsular comandos en protocolos legítimos (HTTP/HTTPS) es una práctica compartida que permite a los 13 grupos identificados evadir las soluciones de seguridad perimetral del sector.

- **Cosechadores de Credenciales (Infostealers):** Se documenta el uso de herramientas comunes para el robo de identidades digitales en equipos de uso público, proporcionando a diversos actores la materia prima necesaria para iniciar sus cadenas de ataque mediante cuentas válidas.

- **Motores de Cifrado para Extorsión:** El uso de variantes de ransomware con estructuras de código similares entre diferentes campañas sugiere una colaboración en el desarrollo o la adquisición de kits de cifrado para impactar la disponibilidad de los datos administrativos.

Nodos aislados o con baja correlación (por ahora):



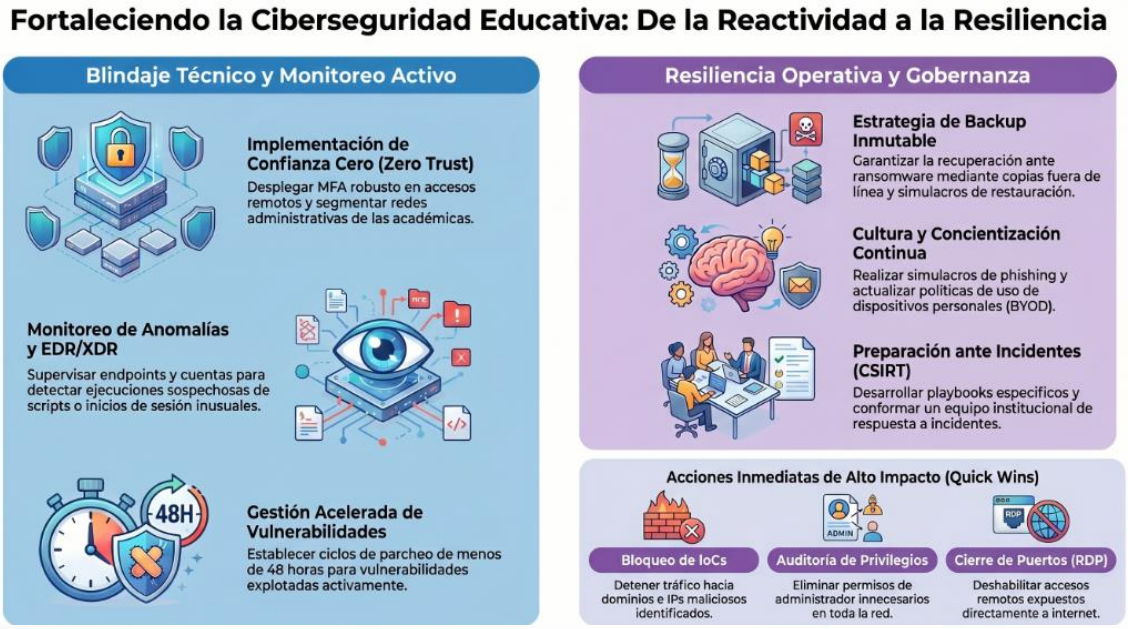
- **Infraestructura de Pruebas o "Staging":** Segmentos de direcciones IP y dominios que muestran actividad de resolución de nombres pero que aún no han sido asociados a la entrega de cargas útiles o exfiltración de datos activa.
- **Hashes de Archivos Huérfanos:** Firmas de archivos detectadas en estaciones de trabajo aisladas que no coinciden con las familias de malware de los grupos principales (como **Mustard Tempest** o **FIN7**) y que carecen de comunicación con la infraestructura de C2 conocida.
- **Servidores de Activos Académicos Legítimos:** Nodos institucionales que, aunque presentan tráfico inusual, este se debe a procesos técnicos internos, migraciones o configuraciones erróneas que no corresponden a patrones de ataque documentados.
- **Cuentas de Usuario con Actividad Anómala Local:** Identidades que muestran intentos de inicio de sesión fallidos, pero cuya telemetría sugiere errores humanos o automatización de servicios internos en lugar de un ataque coordinado de fuerza bruta externa.

- **Dominios de Baja Reputación Sin Actividad de Sector:** FQDNs identificados en listas de bloqueo globales que, si bien son sospechosos, no han intentado interactuar específicamente con la infraestructura educativa colombiana durante el periodo analizado.

- **Indicadores de Compromiso (IoCs) de Campañas Expiradas:** Direcciones IP que pertenecieron a infraestructuras de ataque en el pasado pero que actualmente se encuentran inactivas o han sido reasignadas a servicios legítimos de proveedores de nube.

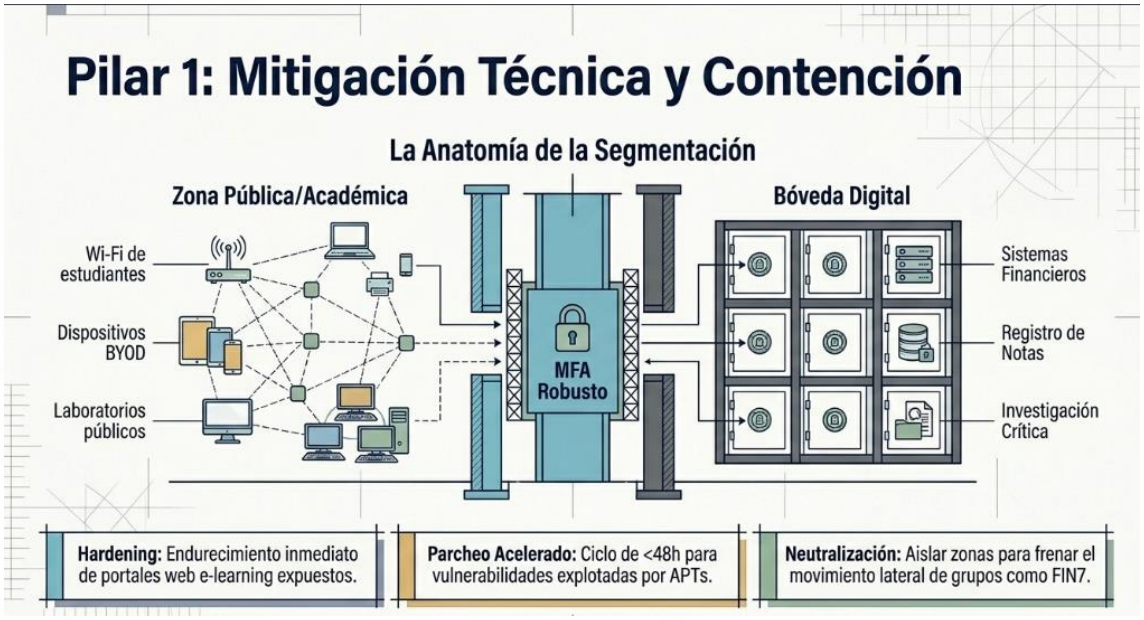
RECOMENDACIONES ESTRATÉGICAS

La gestión del riesgo cibernético en el sector educativo debe evolucionar de un modelo reactivo basado en perímetros hacia un enfoque de **Confianza Cero (Zero Trust)** y visibilidad integral. Es imperativo que las instituciones reconozcan que su infraestructura, compuesta por una mezcla de sistemas administrativos críticos e investigación de alto valor, es un objetivo primario tanto para el cibercrimen financiero como para el espionaje estatal.



La estrategia debe centrarse en la segmentación lógica de redes para aislar los entornos de laboratorios y estudiantes de los servidores que custodian datos sensibles, junto con una inversión prioritaria en la cultura de seguridad de la comunidad académica. Solo mediante la alineación de las capacidades técnicas con una gobernanza sólida se podrá reducir la superficie de ataque y mitigar el impacto de las operaciones coordinadas de los actores de amenaza detectados.

Recomendaciones de Mitigación Técnica



- **Implementación de MFA Robusto:** Desplegar autenticación de múltiples factores en todos los puntos de acceso, especialmente en VPNs y servicios de correo institucional, para neutralizar el uso de cuentas válidas robadas por infostealers.

- **Segmentación de Red Académica vs. Administrativa:** Aislar los segmentos de red de uso público (Wi-Fi de estudiantes y laboratorios) de las zonas que albergan sistemas financieros y de registro, limitando el movimiento lateral de grupos como FIN7.

- **Hardening de Servicios Expuestos:** Realizar un endurecimiento de configuraciones en portales web y plataformas de aprendizaje para mitigar la explotación de aplicaciones públicas.
- **Gestión de Vulnerabilidades Críticas:** Establecer un ciclo de parcheo acelerado (menos de 24-48 horas) para vulnerabilidades conocidas que son explotadas activamente por grupos APT.

Recomendaciones de Detección y Monitoreo

- **Despliegue de Soluciones EDR/XDR:** Monitorear los endpoints para detectar la ejecución de scripts en Python o PowerShell y balizas de Cobalt Strike antes de que se consolide la persistencia.

- **Monitoreo de Anomalías en Cuentas:** Configurar alertas ante comportamientos inusuales de identidad, como inicios de sesión desde ubicaciones geográficas no habituales o en horarios atípicos para el personal docente.

- **Análisis de Tráfico de Red (NTA):** Supervisar el tráfico de salida hacia los 1,202 nodos IP y dominios identificados para detectar canales de comando y control (C2).

- **Auditoría de Logs de Servicios en la Nube:** Centralizar y analizar los registros de acceso a plataformas Office 365 o Google Workspace para identificar exfiltración silenciosa de datos.

Recomendaciones de Resiliencia Operativa

- **Estrategia de Backup Inmutable:** Mantener copias de seguridad fuera de línea o en entornos inmutables para garantizar la recuperación ante ataques de ransomware como los de Mustard Tempest.

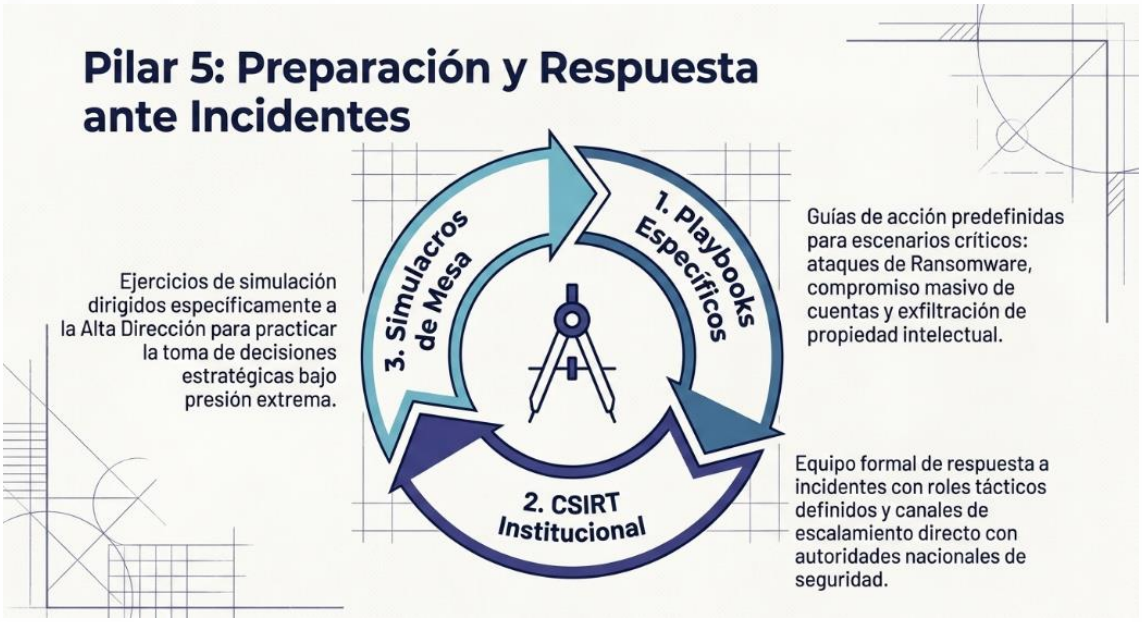
- **Plan de Continuidad Académica:** Definir procedimientos para operar servicios esenciales (clases virtuales, registros de notas) de forma alternativa en caso de una caída masiva de la infraestructura principal.

- **Pruebas de Restauración Periódicas:** Realizar simulacros de recuperación total de sistemas críticos para validar los tiempos de respuesta (RTO) y puntos de recuperación (RPO).

Recomendaciones de Gobernanza

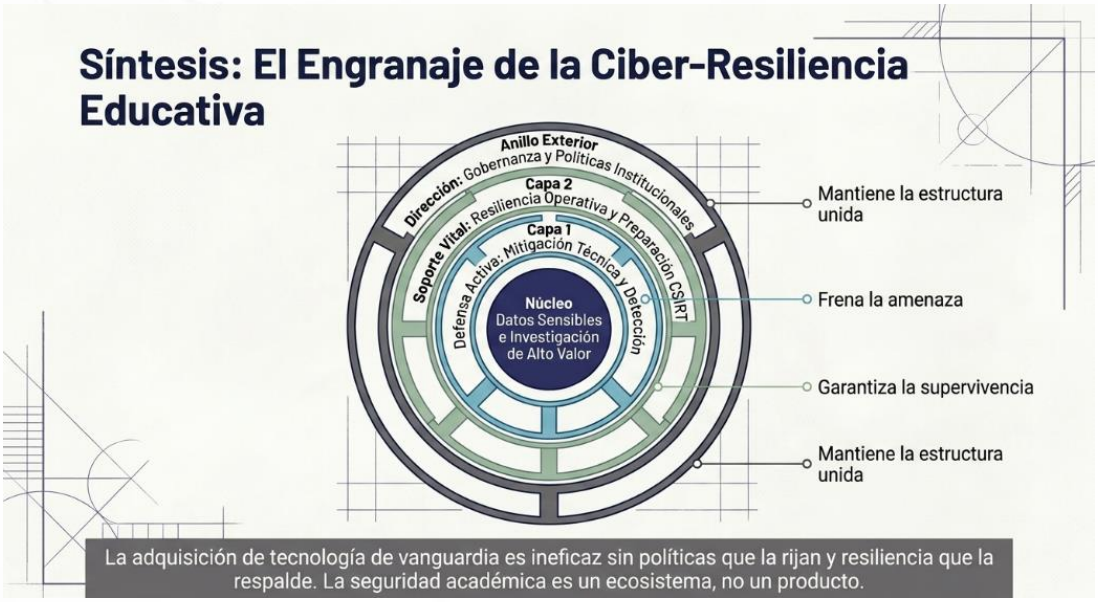
- **Actualización de Políticas de Seguridad:** Formalizar normativas sobre el uso de dispositivos personales (BYOD) y la instalación de software no autorizado en la red institucional.
- **Programa de Concientización Continua:** Ejecutar campañas de simulación de phishing dirigidas a estudiantes y administrativos para reducir la efectividad de los vectores de acceso inicial.
- **Gestión de Riesgos de Terceros:** Evaluar la postura de seguridad de proveedores de servicios tecnológicos y plataformas externas que manejan datos de la institución.

Preparación ante Incidentes



- **Desarrollo de Playbooks Específicos:** Crear guías de respuesta ante incidentes para escenarios de ransomware, compromiso de cuentas y exfiltración de propiedad intelectual.
- **Conformación de un CSIRT Institucional:** Establecer un equipo de respuesta a incidentes con roles definidos y canales de comunicación claros con las autoridades nacionales.
- **Simulacros de Mesa (Tabletop Exercises):** Realizar ejercicios con la alta dirección para practicar la toma de decisiones estratégicas durante una crisis cibernética.

Acciones Inmediatas (Quick Wins)



- **Bloqueo Preventivo de IoCs:** Cargar los dominios e IPs identificados en este informe en las listas de bloqueo de firewalls y proxies institucionales de forma inmediata.
- **Revisión de Privilegios Administrativos:** Auditar y eliminar permisos de administrador innecesarios en estaciones de trabajo y servidores críticos.
- **Cierre de Puertos Críticos (RDP/SMB):** Deshabilitar o proteger tras una VPN cualquier servicio de escritorio remoto o compartido que esté expuesto directamente a internet.
- **Cambio Masivo de Contraseñas en Cuentas Privilegiadas:** Forzar la actualización de credenciales para todas las cuentas con niveles altos de acceso como medida preventiva inicial.

CONCLUSIONES

1. **Convergencia de Actores y Motivaciones:** El sector educación en Colombia no enfrenta una amenaza aislada, sino un ecosistema donde coexisten 13 grupos con objetivos diversos. La infraestructura educativa es un punto de encuentro para el **ciberespionaje estatal (APTs)**, interesado en propiedad intelectual, y el **cibercrimen financiero**, que busca la extorsión mediante ransomware.

2. **Infraestructura Técnica Altamente Reutilizada:** Existe una interdependencia crítica en los recursos de ataque. El uso compartido de los **1,202 nodos IP** y más de **2,400 dominios** demuestra que los atacantes operan bajo una logística centralizada, donde la caída de un solo nodo de control puede afectar la operatividad de múltiples campañas simultáneas.

3. **El Factor Humano como Eslabón Crítico:** El robo de identidades digitales a través de campañas de phishing y el uso de **cuentas válidas (T1078)** es la puerta de entrada principal. Esto indica que los controles perimetrales son insuficientes si no se fortalece la gestión de identidades y la cultura de seguridad de la comunidad académica

4. **Vulnerabilidad del Ecosistema Académico Abierto**: La naturaleza intrínsecamente abierta de las redes universitarias (laboratorios, Wi-Fi público y servicios de educación virtual) ofrece una superficie de ataque extensa. La falta de segmentación robusta entre entornos académicos y administrativos facilita el movimiento lateral de los adversarios hacia servidores críticos.

5. **Estandarización de Herramientas de Post-Explotación**: El uso generalizado de frameworks como **Cobalt Strike** y scripts automatizados en **Python/PowerShell** evidencia que los atacantes han industrializado sus métodos. Esto les permite realizar reconocimientos internos y recolectar datos de forma veloz, reduciendo el tiempo de permanencia necesario para causar daño.

6. **Necesidad Imperativa de un Modelo Zero Trust**: Dado que los controles tradicionales basados en el perímetro están siendo evadidos con éxito, la postura de seguridad del sector debe migrar hacia la verificación continua de cada identidad y dispositivo. La resiliencia

7. operativa dependerá de la capacidad de aislar incidentes mediante segmentación y garantizar la recuperación de datos ante cifrados masivos.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **Adversario (Threat Actor):** Entidad o grupo de individuos motivados que poseen la capacidad y la intención de realizar actividades maliciosas contra una red o sistema.
- **Tácticas, Técnicas y Procedimientos (TTPs):** Describe el "qué", "cómo" y "de qué manera" opera un atacante. Las tácticas son los objetivos, las técnicas son los métodos y los procedimientos son los pasos específicos.
- **Indicadores de Compromiso (IoCs):** Evidencias digitales (como hashes, IPs o dominios) que indican con un alto nivel de confianza que un sistema ha sido vulnerado.
- **Cadenas de Ataque (Kill Chain):** Modelo que describe las fases de un ataque cibernético, desde el reconocimiento inicial hasta la ejecución de los objetivos finales.
- **Movimiento Lateral:** Técnicas que utilizan los atacantes para desplazarse a través de una red después de haber obtenido el acceso inicial, buscando sistemas de mayor valor.
- **Exfiltración de Datos:** Transferencia no autorizada de información desde dentro de una red hacia una ubicación externa controlada por el atacante.

Infraestructura y Redes

- **Comando y Control (C2 / CnC):** Infraestructura (servidores y canales de comunicación) utilizada por los atacantes para enviar instrucciones a los sistemas comprometidos.
- **FQDN (Fully Qualified Domain Name):** Nombre de dominio completo que especifica la ubicación exacta de un host en la jerarquía del DNS.

- **Nodo IP:** Punto de conexión en una red identificado por una dirección IP única. En este contexto, se refiere a los 1,202 puntos de infraestructura detectados.
- **Jump Host (Servidor de Salto):** Equipo intermedio utilizado por los atacantes para saltar de una red a otra o para ocultar su ubicación real de origen.
- **DNS Dinámico (DDNS):** Método para actualizar automáticamente un servidor de nombres en el DNS con la configuración activa de sus nombres de host o direcciones IP.
- **Protocolos de Capa de Aplicación:** Protocolos como HTTP o HTTPS que los atacantes utilizan para "tunelizar" o esconder su tráfico malicioso dentro de tráfico web legítimo.

Herramientas y Malware

- **Ransomware:** Tipo de malware que cifra los archivos de la víctima, exigiendo un rescate económico a cambio de la clave de descifrado.
- **Infostealer:** Software malicioso diseñado específicamente para recolectar y robar información sensible, como credenciales de acceso almacenadas en navegadores.
- **Cobalt Strike:** Herramienta comercial legítima de seguridad (framework de post-explotación) que es frecuentemente abusada por atacantes para mantener el control de redes comprometidas.
- **Hash de Archivo:** Firma digital única (ej. MD5, SHA-256) que identifica de forma inequívoca un archivo malicioso, independientemente de su nombre.
- **Backdoor (Puerta Trasera):** Método para eludir los procedimientos normales de autenticación en un sistema, permitiendo el acceso remoto persistente al atacante.
- **Script de Automatización:** Código escrito generalmente en Python o PowerShell diseñado para ejecutar tareas repetitivas, como el escaneo de redes o la recolección de datos, de forma veloz.

Generales

- **Activos Académicos:** Información que incluye propiedad intelectual, proyectos de investigación científica, patentes y datos personales de la comunidad estudiantil y docente.
- **Comunidad Académica:** Conjunto de usuarios (estudiantes, profesores, administrativos e investigadores) que interactúan con la infraestructura tecnológica de la institución.
- **Postura de Seguridad Institucional:** El estado de preparación y defensa de una universidad o centro educativo frente a las amenazas identificadas en el entorno colombiano.
- **Propiedad Intelectual (PI):** Creaciones de la mente, como invenciones científicas o desarrollos de software, que son el objetivo principal de los grupos de ciberespionaje.
- **Infraestructura de Educación Virtual:** Plataformas y servidores (como LMS o portales de notas) que permiten la continuidad de las actividades académicas y que son críticos para la resiliencia operativa.

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