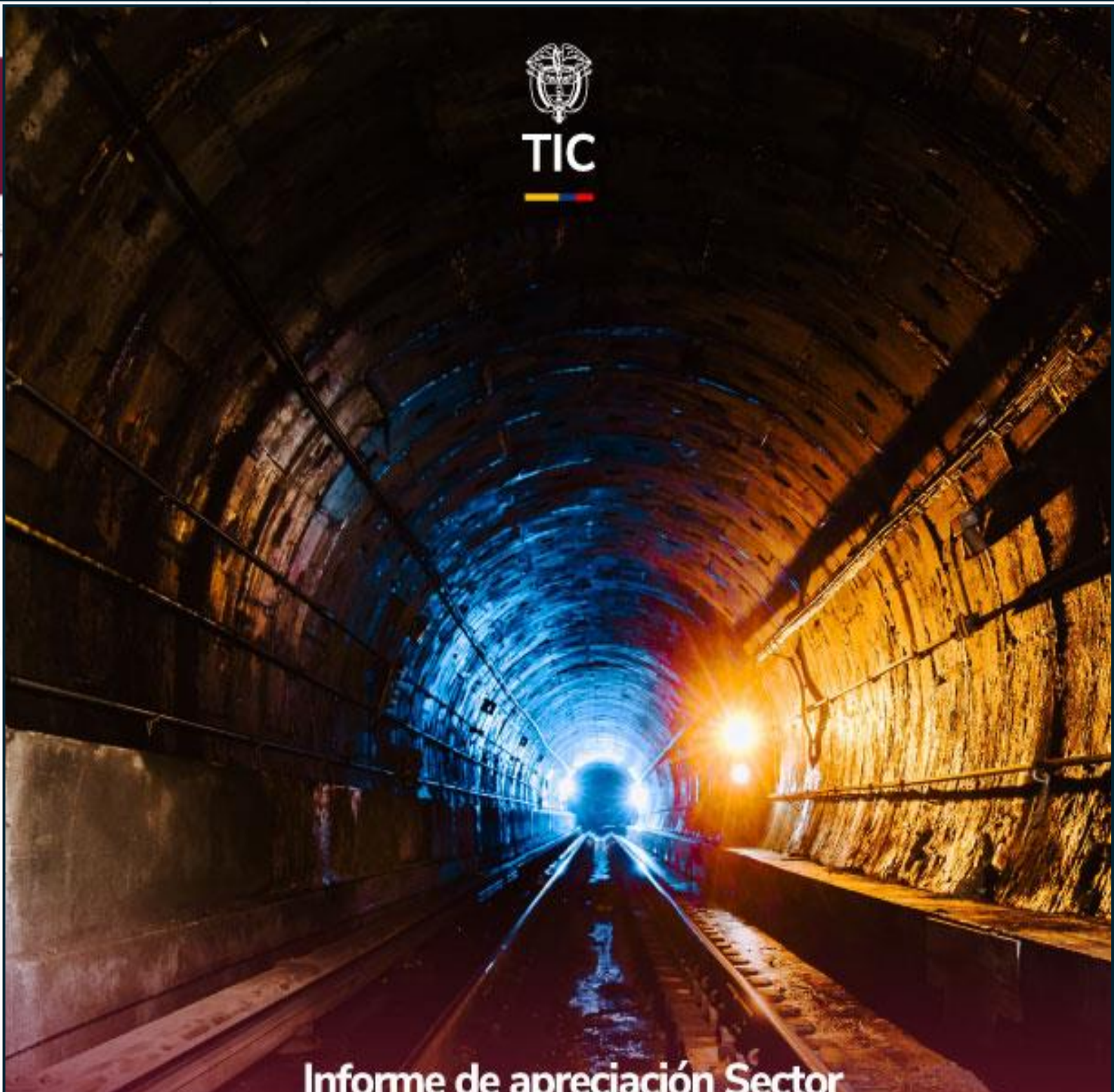
TIC



Informe de apreciación Sector

Minería

COLCERT

Contenido

RESUMEN EJECUTIVO 4
INTRODUCCIÓN 5
Hallazgos Clave 6
Conclusión Estratégica 8
OBJETIVO Y ALCANCE 9
Objetivo 9
Alcance 9
CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR 10
Definición y Entendimiento del Sector 10
Superficie de Ataque 10
PANORAMA ACTUAL DE AMENAZAS 12
Tipología de Eventos Identificados 14
INDICADORES DE COMPROMISO (IoCs) 17
Resumen de IoCs Relevantes 19
ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES) 21
Identificación de Actores Relevantes 21
Objetivos y Sectores Target 23
Campañas Activas 26
TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs) 28
Mapeo a MITRE ATT&CK Framework 28
Cadenas de Ataque Observadas 28
Cadenas de ataque: 30
Herramientas y Malware Específico 32
CORRELACIÓN ENTRE ACTORES Y GRUPOS 34
Infraestructura Compartida 34
Herramientas y TTPs Comunes 35
Posibles Colaboraciones o Vínculos 36
Visualización de Relaciones 37
Relaciones directas documentadas: 38

Relaciones por infraestructura compartida 39
Relaciones por herramientas comunes 40
Nodos aislados o con baja correlación (por ahora): 41
RECOMENDACIONES ESTRATÉGICAS 42
Recomendaciones de Mitigación Técnica 42
Recomendaciones de Detección y Monitoreo 43
Recomendaciones de Resiliencia Operativa 44
Recomendaciones de Gobernanza 45
Preparación ante Incidentes 46
Acciones Inmediatas (Quick Wins) 47
CONCLUSIONES 48
GLOSARIO 50
Conceptos de Inteligencia y Amenazas 50
Infraestructura y Redes 50
Herramientas y Malware 51
Sector 51

Informe de apreciación
Sector Minería

COLCERT IN- 20260706-037

TLP: CLEAR

RESUMEN EJECUTIVO

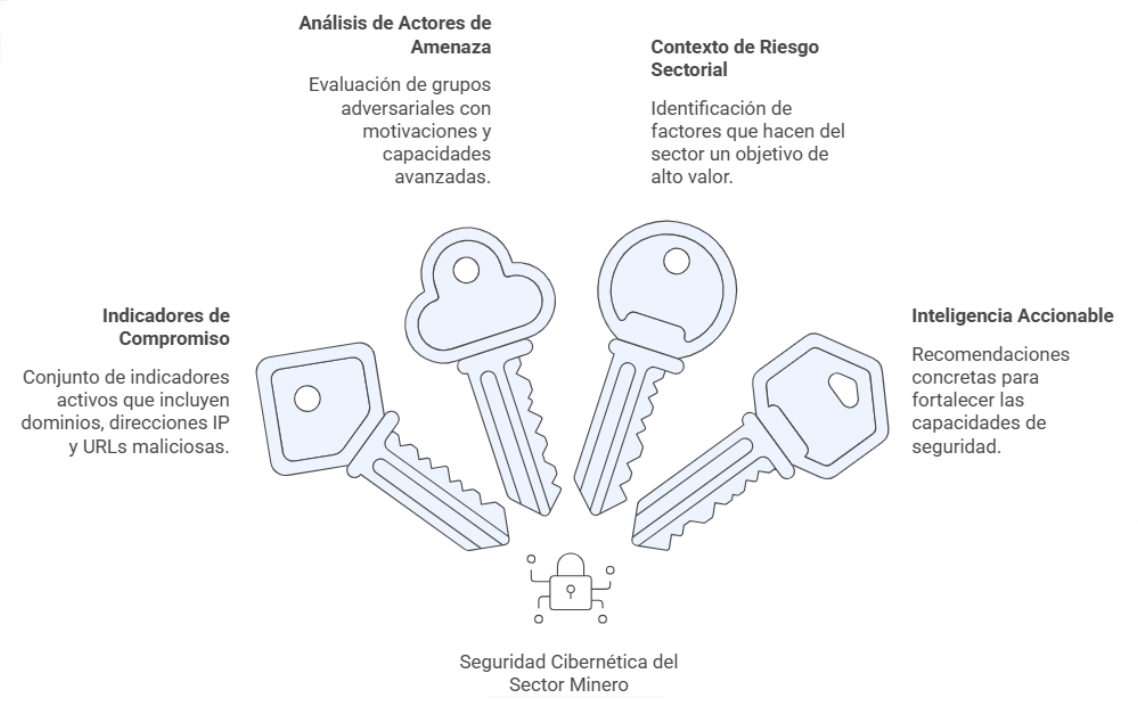
El sector defensa colombiano enfrenta un panorama de amenazas cibernéticas de creciente complejidad, impulsado por la actividad de actores con capacidades avanzadas y motivaciones que trascienden el ámbito del crimen común para adentrarse en operaciones de espionaje estatal, sabotaje de infraestructura crítica y desinformación estratégica. La inteligencia recopilada durante el período analizado confirma la presencia de actividad adversarial activa con capacidad de impacto directo sobre instituciones, sistemas y personal vinculado al sector defensa en Colombia. El presente informe tiene como propósito documentar y contextualizar dicha actividad, proporcionando elementos de juicio sólidos que orienten las decisiones estratégicas y operativas en materia de seguridad digital para el sector minero en Colombia.

- **Base de indicadores de compromiso:** Conjunto de 3.343 indicadores activos que incluyen dominios, direcciones IP, hashes de archivos y URLs maliciosas, recopilados entre el 17 de abril y el 5 de mayo de 2026.
- **Análisis de actores de amenaza:** Evaluación de nueve grupos adversariales con referencias confirmadas a Colombia, abarcando sus motivaciones, capacidades y vectores de ataque más relevantes para el entorno del sector defensa.
- **Contexto de riesgo sectorial:** Identificación de los factores que hacen del sector defensa colombiano un objetivo de alto valor estratégico, considerando la naturaleza de su información, sus operaciones y su infraestructura tecnológica.
- **Inteligencia accionable:** Traducción de los hallazgos técnicos en recomendaciones concretas orientadas a fortalecer las capacidades de detección, respuesta y prevención en las organizaciones del sector.

Informe de apreciación Sector Minería

COLCERT IN- 20260706-037

TLP: CLEAR



INTRODUCCIÓN

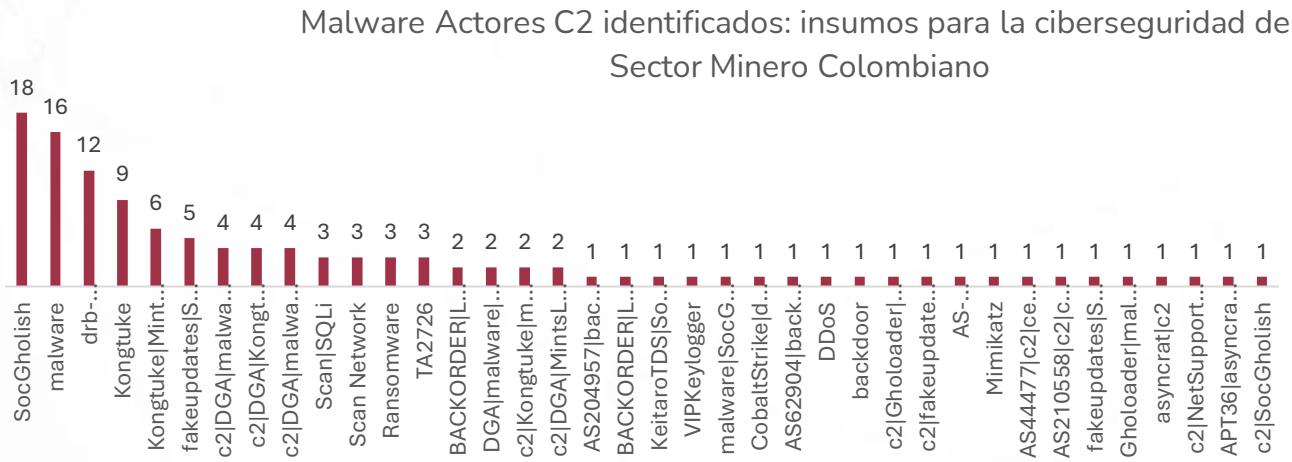
El panorama de amenazas para el sector minero en Colombia durante el periodo actual muestra una actividad significativa por parte de grupos de actores con diversas motivaciones, que van desde el espionaje estatal hasta el beneficio económico a través de ataques de extorsión. La importancia estratégica de la infraestructura minero-energética del país la convierte en un objetivo prioritario para campañas dirigidas que buscan comprometer la confidencialidad de la información operativa y la disponibilidad de los servicios críticos. Se observa una convergencia de adversarios con historial de ataques a infraestructuras críticas y sectores gubernamentales, lo que eleva el riesgo de incidentes con impacto nacional.

Puntos Clave:

- Identificación de múltiples actores con presencia activa y dirigida hacia objetivos dentro del territorio colombiano.

- Persistencia de grupos vinculados a operaciones de ciberespionaje de largo alcance.
- Presencia de actores especializados en el despliegue de software malicioso para la interrupción de procesos industriales y financieros.
- Alta correlación entre la actividad de grupos internacionales de amenazas avanzadas y la infraestructura del sector minero nacional.
- Diversificación de los vectores de ataque utilizados para el compromiso inicial y la exfiltración de datos sensibles.
- Necesidad de reforzar la vigilancia ante actores con capacidades probadas en la afectación de sectores de transporte, salud y gobierno en la región.

Hallazgos Clave



Hallazgos Clave

- Se identificaron **3.347 indicadores de compromiso activos** en el período enero 2025 – mayo 2026, todos en estado activo al momento del análisis.

- El tipo de indicador más frecuente son los dominios maliciosos (FQDN) con **1.570 registros (46,9%)**, seguidos de direcciones IP comprometidas con **1.225 registros (36,6%)**, evidenciando infraestructura activa de comando y control.

- Se detectaron **137 indicadores de alta severidad** (puntuación ≥13), concentrados principalmente en direcciones IP, representando el subconjunto de mayor riesgo inmediato para el sector.

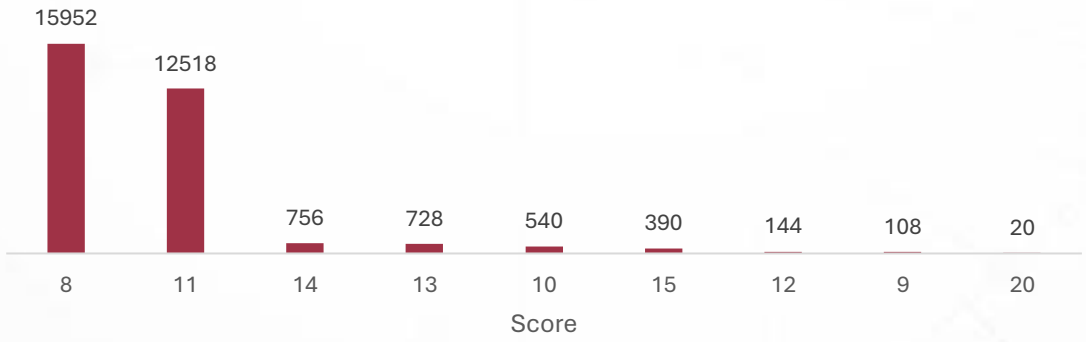
- **16 grupos adversarios** con capacidades avanzadas fueron identificados en el panorama de amenazas, con motivaciones que abarcan espionaje industrial, extorsión económica y sabotaje de infraestructura crítica.

- Tres grupos adversarios —**APT34, FIN7 y UNC1543**— registran vínculos documentados directamente con Colombia, con actividad reciente actualizada entre el 1 y el 3 de mayo de 2026, indicando campañas en curso.

- **APT44 (Sandworm)** representa el actor de mayor riesgo para infraestructura operacional, con historial documentado de ataques destructivos contra sectores Minero y energéticos.

- El **100% de los indicadores** se encuentran vigentes con fechas de expiración proyectadas entre mayo y julio de 2026, confirmando que la amenaza es activa y no residual.

Score de riezgo por etiqueta (8-20) - Sector Minero de Colombia



Recomendaciones Prioritarias

- Implementar de forma inmediata los 3.343 indicadores de compromiso activos en las soluciones de detección perimetral y de endpoints en todas las organizaciones del sector defensa.

- Reforzar los controles sobre tráfico saliente hacia dominios de reciente registro y con patrones de nomenclatura evasivos, priorizando la revisión de los 1.570 dominios identificados en el presente análisis.

- Intensificar la vigilancia sobre comunicaciones electrónicas que contengan adjuntos ejecutables o enlaces a dominios no verificados, dado que el phishing dirigido representa el principal vector de entrada contra objetivos del sector defensa.

- Establecer un proceso de actualización continua de la lista de indicadores, considerando que los plazos de expiración oscilan entre 30 y 60 días, para garantizar la vigencia permanente de las capacidades de detección.

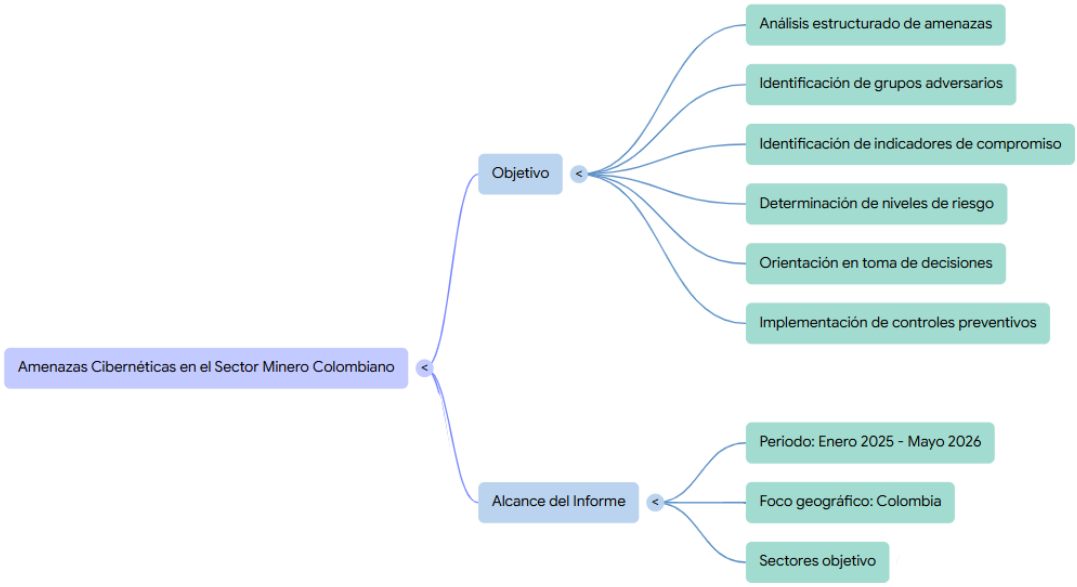
- Desarrollar programas de concienciación en ciberseguridad dirigidos al personal militar, civil y contratista del sector, con énfasis en el reconocimiento de tácticas de ingeniería social e intentos de suplantación de identidad.

- Priorizar el monitoreo de indicadores con puntuación de riesgo 11, los cuales representan las amenazas de mayor severidad y confiabilidad dentro del conjunto analizado, con especial atención sobre activos críticos del sector minero de Colombia.

Conclusión Estratégica

El sector minero colombiano enfrenta un panorama de amenaza activo y multidimensional. La convergencia de actores estatales con capacidades destructivas, grupos financieramente motivados con historial en sectores de infraestructura, y una infraestructura maliciosa de gran escala con más de 3.300 indicadores vigentes, configura un riesgo elevado que requiere respuesta inmediata y sostenida. La presencia explícita de Colombia en el perfil de tres grupos adversarios refuerza la necesidad de tratar estas amenazas como objetivos dirigidos y no como exposición incidental. Una postura de ciberseguridad reactiva resulta insuficiente ante este nivel de actividad; se requiere una estrategia proactiva basada en inteligencia de amenazas, respuesta coordinada y protección de activos críticos operacionales.

OBJETIVO Y ALCANCE



Objetivo

Proporcionar al sector minero colombiano un análisis estructurado del panorama de amenazas cibernéticas vigentes, identificando los grupos adversarios activos, los indicadores de compromiso asociados y el nivel de riesgo que representan para las operaciones del sector, con el fin de orientar la toma de decisiones en materia de ciberseguridad y la implementación de controles preventivos y de respuesta.

Alcance

El presente informe cubre el análisis de 3.347 indicadores de compromiso activos recopilados entre enero de 2025 y mayo de 2026, asociados a 16 grupos adversarios identificados mediante inteligencia de amenazas de fuentes especializadas. El análisis contempla indicadores de tipo FQDN, dirección IP, hashes de archivo (MD5, SHA-1, SHA-256) y URLs maliciosas, todos en estado activo al momento de la elaboración de este informe. El enfoque está dirigido a las operaciones del sector minero en Colombia, con especial atención a los actores que registran vínculos documentados con el país y a aquellos con historial de ataques contra infraestructura crítica, sector minero e industria extractiva a nivel regional y global.

Informe de apreciación
Sector Minería

COLCERT IN- 20260706-037

TLP: CLEAR

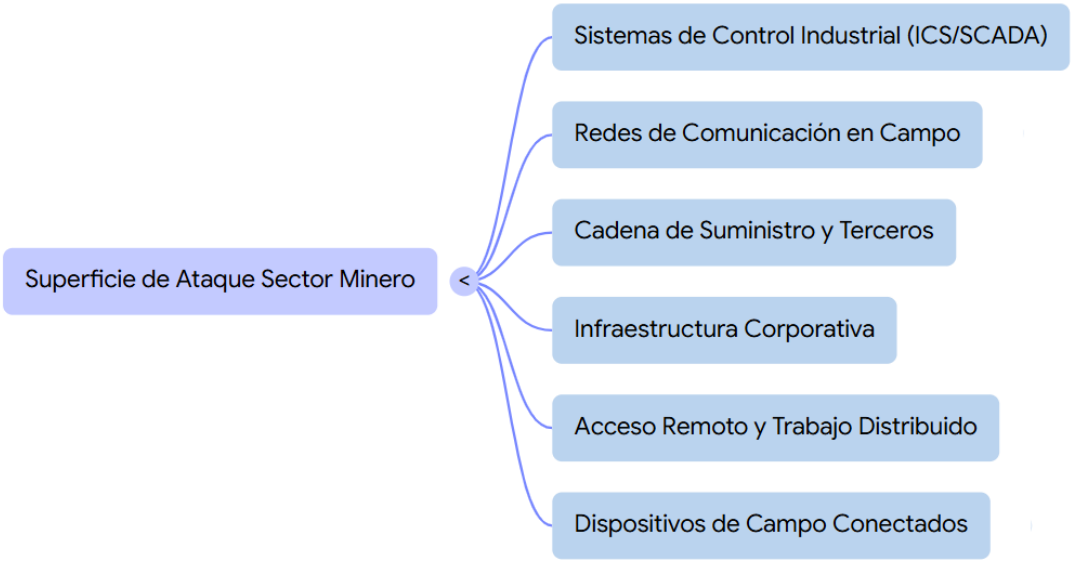
CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR

Definición y Entendimiento del Sector

El sector minero colombiano constituye uno de los pilares fundamentales de la economía nacional, representando una fuente significativa de exportaciones y generación de divisas. Colombia cuenta con una amplia variedad de recursos minerales, entre los que se destacan el carbón, el oro, el níquel, las esmeraldas y los minerales estratégicos emergentes como el cobre y el litio. Las operaciones del sector abarcan desde la exploración y extracción hasta el procesamiento, transporte y comercialización de minerales, involucrando tanto a grandes empresas multinacionales como a operadores medianos y pequeños distribuidos a lo largo del territorio nacional. En los últimos años, el sector ha acelerado su proceso de transformación digital, incorporando tecnologías de automatización, monitoreo remoto, sistemas de control industrial y conectividad en sitios de operación que históricamente permanecían aislados. Esta convergencia entre tecnología de información (TI) y tecnología operacional (OT) ha incrementado significativamente la eficiencia productiva, pero al mismo tiempo ha ampliado la superficie de exposición a amenazas cibernéticas, convirtiendo al sector en un objetivo de creciente interés para actores maliciosos con motivaciones económicas, geopolíticas y de sabotaje.

Superficie de Ataque

El proceso de digitalización del sector minero ha generado un ecosistema tecnológico complejo y heterogéneo, donde coexisten sistemas heredados con plataformas modernas conectadas, creando múltiples puntos de entrada susceptibles de ser explotados por actores maliciosos. A continuación, se describen los principales componentes que conforman la superficie de ataque del sector:



- **Sistemas de Control Industrial (ICS/SCADA):** Plataformas utilizadas para la supervisión y control de procesos extractivos, equipos de perforación, sistemas de ventilación en minería subterránea y transporte de minerales. Muchos de estos sistemas fueron diseñados sin consideraciones de seguridad cibernética y operan con protocolos propietarios de difícil actualización.

- **Redes de comunicación en campo:** Infraestructura de conectividad desplegada en zonas remotas mediante enlaces satelitales, redes privadas y comunicaciones inalámbricas industriales, las cuales presentan mayores dificultades de monitoreo y control en comparación con entornos corporativos tradicionales.

- **Cadena de suministro y proveedores terceros:** Contratistas, proveedores de equipos y empresas de mantenimiento que acceden de forma remota o física a los sistemas de las operaciones mineras, representando un vector de entrada frecuentemente subestimado en los modelos de gestión de riesgo.

- **Infraestructura corporativa y sistemas de gestión:** Plataformas ERP, sistemas de gestión de producción, herramientas de planificación y aplicaciones de negocio que concentran información crítica sobre reservas, producción, contratos y datos financieros, siendo objetivos primarios para campañas de espionaje y ransomware.

- **Acceso remoto y trabajo distribuido:** Conexiones VPN, escritorios remotos y plataformas de colaboración utilizadas por equipos de operación, ingeniería y administración, que si no están debidamente configuradas representan una puerta de entrada directa a la red interna de la organización.

- **Dispositivos de campo y equipos conectados:** Sensores IoT industriales, drones de monitoreo, vehículos autónomos y equipos de medición conectados a redes corporativas, cuya gestión de seguridad frecuentemente queda por fuera de los programas de parchado y actualizaciones convencionales.

PANORAMA ACTUAL DE AMENAZAS

El sector minero en Colombia y América Latina atraviesa uno de los momentos de mayor exposición cibernética de su historia. Los ataques dirigidos al sector minero en la región han registrado un incremento sostenido, con una velocidad de intrusión que plantea retos críticos para los tiempos de respuesta de las organizaciones afectadas. Este fenómeno no es aislado: las amenazas cibernéticas están evolucionando y escalando a un ritmo alarmante para las empresas de minería y metales, haciendo indispensable comprender el panorama de riesgo actual y las amenazas que introducen las nuevas tecnologías, como condición previa para mantener operaciones confiables y resilientes. Un factor determinante en este escalonamiento es la naturaleza estratégica de los recursos que Colombia extrae: el litio, el cobre y otros minerales críticos han convertido a la minería latinoamericana en un blanco de alto valor para actores maliciosos, quienes reconocen el peso geopolítico y económico de estas materias primas en el contexto de la transición energética global. A esto se suma que la ciberseguridad en la minería enfrenta riesgos específicos derivados de la convergencia entre entornos digitales y operacionales, lo que exige la adopción de buenas prácticas orientadas a la protección integral de las operaciones mineras.

Informe de apreciación
Sector Minería

COLCERT IN- 20260706-037

TLP: CLEAR

TITULO	FECHA	FUENTE / ENLACE
Ciberataques dirigidos al sector minero se duplican: escenario en minería latinoamericana y Colombia	2026-03-11	Acsis.org
El 60% de ciberataques en minería apunta a minerales críticos (incl. Colombia y Latam)	2026-03-05	Rumbominero
Litio, cobre y ciberdelincuencia: por qué la minería latinoamericana se convirtió en blanco (incluye contexto colombiano)	2026-03-10	sercolombiano.com
Ciberseguridad en la minería: riesgos y buenas prácticas para protección de operaciones mineras	2025-03-27	commit.works
Ciberataques a minería de Latam: no solo volumen, sino velocidad de respuesta (análisis aplicable a sector minero en Colombia)	2026-03-11	ey.com

El registro de incidentes de ciberseguridad del sector Minas y Energía en Colombia comprende 34 eventos documentados entre mayo de 2020 y noviembre de 2025, consolidando un histórico de cinco años que refleja una actividad maliciosa sostenida y con tendencia creciente sobre este sector estratégico. La distribución temporal es reveladora: mientras en el período 2020–2022 se registraron 10 incidentes, el bienio 2024–2025 concentró 22 eventos, lo que representa más del doble, evidenciando una escalada significativa en la frecuencia de ataques. Geográficamente, Bogotá D.C. concentra el 91% de los incidentes, lo que refleja la centralización de los sistemas de información y gobierno del sector en la capital, aunque también se registraron eventos en Antioquia, Risaralda, Tolima y Boyacá, indicando que la amenaza no es exclusiva del nivel central. En cuanto a la tipología, el fraude es la categoría más frecuente con 16 incidentes, siendo el phishing y la suplantación los vectores predominantes, seguido por el compromiso de información con 9 eventos, la mayoría clasificados como graves.

Fecha	Calificación	Tipo de Incidente	Descripción	Importancia (Análisis)
2022 Sep 22	Muy Grave	Compromiso de Información	Acceso no Autorizado a Información	Único incidente clasificado como Muy Grave en todo el histórico. Representa el evento de mayor severidad registrado en el sector, con potencial de exfiltración de información sensible a nivel nacional.
2020 Nov 10	Grave	Disponibilidad	Interrupciones	Afectación directa a la continuidad operacional del sector a nivel nacional. Las interrupciones en sistemas críticos de Minas y Energía pueden impactar cadenas productivas y servicios esenciales.
2024 Dec 06	Grave	Intrusión	Compromiso de Aplicaciones	Intrusión confirmada sobre aplicaciones del sector con alcance nacional. Este vector es frecuentemente utilizado como punto de entrada para movimientos laterales y despliegue de malware.
2024 May 31	Grave	Intrusión	Compromiso de Cuenta con Privilegios	Compromiso de credenciales con privilegios elevados, lo que otorga al atacante capacidad de control sobre sistemas críticos y facilita la persistencia dentro de la infraestructura comprometida.
2025 Nov 24	Grave	Sistema Vulnerable	Sistema Vulnerable	Exposición activa de sistemas sin remediar en el periodo más reciente del histórico, indicando que persisten brechas de gestión de vulnerabilidades en la infraestructura del sector a nivel nacional.

Los incidentes de intrusión, que incluyen compromiso de aplicaciones y compromiso de cuentas con privilegios, así como los sistemas vulnerables expuestos, configuran el subconjunto de mayor riesgo operacional dado su potencial de impacto sobre la continuidad y la integridad de los sistemas críticos del sector. Cabe destacar que el único incidente clasificado como **Muy Grave** corresponde a un acceso no autorizado a información registrado en septiembre de 2022, mientras que los incidentes de disponibilidad —con interrupciones documentadas en 2020— señalan antecedentes de afectación directa a la operación. Este historial, analizado en conjunto con el panorama de amenazas vigente, subraya que el sector no enfrenta un riesgo hipotético sino una realidad documentada y en aceleración.

Tipología de Eventos Identificados

El análisis de los 3.347 indicadores de compromiso activos asociados al sector minero colombiano revela un ecosistema de amenazas diverso y técnicamente sofisticado, donde cada tipo de indicador cumple un rol específico dentro de las cadenas de ataque identificadas. Los dominios maliciosos representan el vector de mayor volumen, siendo utilizados tanto para infraestructura de comando y control como para operaciones de phishing dirigido, patrón consistente con los grupos adversarios identificados —especialmente FIN7, FIN11 y APT34— que históricamente despliegan infraestructura de red extensa antes de ejecutar sus campañas. Las direcciones IP comprometidas, segundo componente en volumen, concentran la mayor proporción de indicadores de alta severidad (puntuación ≥13), lo que sugiere servidores activamente utilizados para operaciones en curso más que infraestructura residual. Los indicadores de archivo —MD5, SHA-1 y SHA-256— con distribución relativamente equilibrada entre sí, apuntan a familias de malware asociadas a los grupos identificados, incluyendo herramientas de acceso remoto, stealers y componentes de ransomware documentados en campañas previas de FIN6, FIN7 y UNC1543. Finalmente, las URLs maliciosas, aunque menores en volumen, representan puntos de entrega directa de payloads o páginas de captura de credenciales, reforzando el patrón de phishing dirigido evidenciado también en el registro histórico de incidentes del sector, donde esta modalidad acumula la mayor frecuencia de eventos documentados entre 2020 y 2025.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector Minero
FQDN (Dominios)	1.570	Google Threat Intelligence, MISP Import	**Alta** — Infraestructura de C2, phishing dirigido y dominios que suplantan servicios corporativos legítimos utilizados en entornos mineros
IP Address	1.225	Google Threat Intelligence, MISP Import, abuse.ch	Crítica — Concentra los indicadores de mayor severidad (score ≥13); servidores activos en campañas en curso contra infraestructura crítica
SHA-256	177	Google Threat Intelligence, AlienVault OTX	**Alta** — Hashes de malware asociados a grupos con historial en sectores industriales y minero-energéticos; incluye ransomware y RATs
MD5	174	Google Threat Intelligence, abuse.ch ThreatFox	Media-Alta — Variantes de herramientas maliciosas conocidas; útiles para correlación con incidentes históricos del sector
SHA-1	172	Google Threat Intelligence, MISP Import	**Media-Alta** — Complementarios a SHA-256 para identificación de artefactos maliciosos en endpoints y sistemas OT
URL	29	Google Threat Intelligence, abuse.ch URLhaus	**Alta** — Puntos de entrega de payloads y páginas de captura de credenciales; directamente vinculadas al vector de phishing dominante en el histórico de incidentes

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

Análisis de la Distribución de Amenazas

- Predominio de infraestructura de red sobre artefactos de archivo: El 83,5% de los indicadores corresponde a componentes de red (FQDN + IP Address), mientras que los indicadores de archivo (hashes) representan solo el 15,6%. Esta distribución indica que los grupos adversarios identificados priorizan el despliegue y mantenimiento de infraestructura de comunicación activa sobre la distribución masiva de malware, comportamiento característico de actores con objetivos de espionaje prolongado y acceso persistente, como APT34 y APT44.

- Concentración geográfica del riesgo en Bogotá D.C.: El 91% de los incidentes históricos del sector se registraron en la capital, donde se concentran los sistemas de gestión, información corporativa y plataformas de gobierno del sector. Esta centralización convierte a los activos TI bogotanos en el objetivo primario de cualquier campaña dirigida al sector minero colombiano.

- Escalada sostenida en frecuencia de incidentes: El histórico de incidentes muestra una duplicación en la frecuencia entre los períodos 2020–2022 y 2024–2025, pasando de 10 a 22 eventos documentados. Esta tendencia es coherente con el incremento global de ataques al sector reportado para Latinoamérica en 2026, donde los ciberataques dirigidos a minería se han duplicado según fuentes especializadas del sector.

- Fraude como vector de entrada predominante: El 47% de los incidentes históricos corresponde a fraude, con phishing y suplantación como técnicas dominantes. Este patrón es consistente con la infraestructura de dominios maliciosos identificada en los IOCs, donde se detectaron dominios que suplantan servicios de actualización de sistema, Microsoft y Adobe, plataformas ampliamente utilizadas en entornos corporativos mineros.

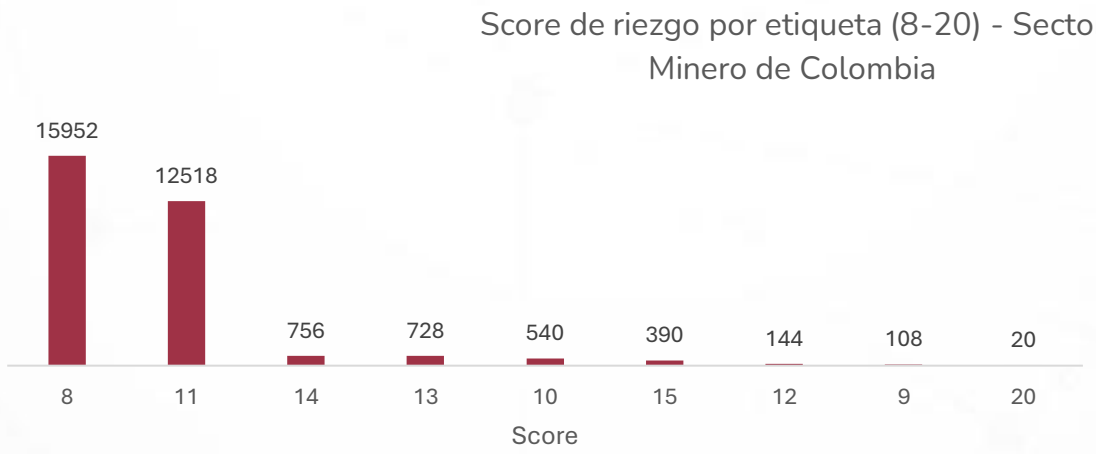
- Incidentes graves superan a los menores en impacto real: Aunque los incidentes clasificados como menores son frecuentes en tipología de fraude, los eventos de mayor consecuencia operacional —compromiso de información, intrusiones y sistemas vulnerables— están clasificados en su totalidad como graves o muy graves, con un único evento de clasificación máxima registrado en 2022 correspondiente a acceso no autorizado a información.

- Mineralidad crítica como factor amplificador del riesgo: La exposición de Colombia en litio, cobre, oro y carbón la posiciona como objetivo de actores con motivaciones geopolíticas y económicas simultáneas. Grupos como APT34, con nexo a intereses estatales en recursos minero-energéticos, y FIN7, orientado a extracción financiera en sectores de infraestructura, representan amenazas cuya motivación está directamente alineada con el perfil productivo del sector minero nacional.

- Indicadores de alta severidad concentrados en IPs: Los 137 indicadores con puntuación ≥13 son predominantemente direcciones IP, lo que sugiere la existencia de servidores dedicados y activos para operaciones en curso. Esta característica eleva la urgencia de implementar controles de bloqueo y monitoreo sobre este subconjunto específico de manera prioritaria frente al resto del universo de IOCs.

INDICADORES DE COMPROMISO (IoCs)

El presente capítulo documenta y analiza el conjunto de indicadores de compromiso recopilados durante el período enero 2025 – mayo 2026, los cuales constituyen la base técnica de inteligencia sobre la que se fundamentan las evaluaciones de riesgo y las recomendaciones defensivas de este informe. Los 3.347 indicadores activos identificados fueron obtenidos a través de múltiples fuentes de inteligencia de amenazas de reconocimiento internacional, correlacionados con los grupos adversarios de mayor relevancia para el sector minero colombiano y validados en cuanto a su vigencia y nivel de confiabilidad. Cada indicador representa una evidencia técnica concreta de infraestructura maliciosa, artefactos de ataque o puntos de comunicación utilizados por actores de amenaza en campañas activas, por lo que su tratamiento no debe limitarse a la consulta referencial, sino que debe traducirse en acciones de detección, bloqueo y monitoreo dentro de los entornos tecnológicos del sector. La totalidad de los indicadores se encuentra en estado activo con fechas de expiración proyectadas entre mayo y julio de 2026, lo que confirma su vigencia operacional al momento de la publicación de este informe.



Análisis Cuantitativo de Inteligencia

- **Volumen total de indicadores:** Se identificaron 3.347 indicadores de compromiso activos, distribuidos en seis tipos: FQDN (1.570), IP Address (1.225), SHA-256 (177), MD5 (174), SHA-1 (172) y URL (29), configurando un universo de inteligencia de cobertura amplia sobre infraestructura de red y artefactos maliciosos.

- **Distribución por nivel de severidad:** El sistema de puntuación empleado clasifica los indicadores en rangos que van desde score 8 hasta score 20. La distribución muestra que 1.994 indicadores (59,6%) se encuentran en score 8, representando amenaza confirmada; 1.138 indicadores (34%) alcanzan score 11, indicando mayor nivel de corroboración; y 137 indicadores (4,1%) superan el umbral de score 13, siendo clasificados como de alta severidad. Solo 1 indicador alcanzó la puntuación máxima de 20, correspondiente a una amenaza con el más alto nivel de confirmación y peligrosidad.

- **Indicadores de alta severidad:** Los 137 indicadores con puntuación ≥13 están compuestos principalmente por direcciones IP con corroboración multifuente, siendo validados simultáneamente por Google Threat Intelligence, MISP Import e indicadores de inteligencia propios. Este subconjunto representa el bloque de acción inmediata prioritaria para los equipos de seguridad del sector.

- **Cobertura temporal:** El período de recopilación abarca desde enero de 2025 hasta el 4 de mayo de 2026, con una concentración de nuevos indicadores en las semanas del 26 de abril al 4 de mayo de 2026, lo que refleja campañas activas en curso durante el período de análisis inmediatamente previo a la publicación de este informe.

- **Fuentes de inteligencia:** Google Threat Intelligence es la fuente con mayor cobertura, presente en la totalidad de los 3.347 indicadores. MISP Import contribuye con corroboración en 1.127 indicadores (33,7%), mientras que abuse.ch ThreatFox aporta contexto sobre 93 indicadores vinculados a familias de malware específicas. AlienVault OTX Pulse cubre 88 indicadores y CISA Reports respalda 2 indicadores de origen gubernamental estadounidense, los de mayor nivel de atribución formal.

- **Vigencia operacional:** El 100% de los indicadores se encuentra en estado activo. Las fechas de expiración se distribuyen entre el 14 de mayo de 2026 y el 3 de julio de 2026, con la mayoría concentrada en junio de 2026, confirmando que la ventana de riesgo operacional es inmediata y no proyectada.

- **Indicadores con múltiples fuentes de validación:** Un subconjunto de indicadores cuenta con validación simultánea de tres o más fuentes independientes —Google Threat Intelligence, MISP Import y Google Threat Intelligence Indicators—, lo que eleva significativamente su nivel de confiabilidad y reduce la probabilidad de falsos positivos al momento de implementar controles de bloqueo.

Resumen de IoCs Relevantes

La siguiente tabla sintetiza los componentes de inteligencia de mayor relevancia estratégica para el sector minero colombiano, agrupando los indicadores según su naturaleza técnica, función dentro de las cadenas de ataque identificadas y nivel de riesgo asociado. Esta síntesis está orientada a facilitar la priorización de controles por parte de los equipos de seguridad, estableciendo una jerarquía de atención basada en el impacto potencial de cada componente sobre los activos críticos del sector. Los niveles de riesgo asignados integran tanto la puntuación de los indicadores como el contexto de los grupos adversarios a los que se encuentran asociados y el historial de incidentes documentado para el sector.

Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Direcciones IP de alta severidad (score ≥13)	137 IPs con validación multifuente activas en infraestructura de C2 y operaciones en curso. Concentran el mayor nivel de corroboración del conjunto total de IOCs.	Crítico
Dominios que suplantan servicios legítimos	FQDNs que imitan plataformas corporativas como Microsoft, Adobe, actualizaciones de sistema y servicios cloud. Diseñados para operaciones de phishing dirigido y entrega de payloads.	Alto
Hashes de malware con validación abuse.ch	93 indicadores respaldados por abuse.ch ThreatFox, asociados a familias de malware con capacidades de acceso remoto, robo de credenciales y movimiento lateral documentadas en entornos industriales.	Alto
URLs de entrega de payloads	29 URLs activas utilizadas como puntos de distribución de malware o captura de credenciales. Vector directamente vinculado al patrón de phishing dominante en el histórico de incidentes del sector.	Alto
Indicadores validados por CISA	2 indicadores con respaldo gubernamental formal de CISA, que implican atribución de alto nivel de confianza a actores con capacidades avanzadas y objetivos sobre infraestructura crítica.	Alto
Dominios de infraestructura C2 activa	FQDNs registrados recientemente con patrones de nomenclatura técnica asociados a herramientas de post-explotación utilizadas por APT34, FIN7 y grupos afines.	Alto
IPs en rango score 11 con doble fuente	1.138 direcciones IP con corroboración de Google Threat Intelligence y MISP Import simultáneamente, que representan infraestructura de apoyo a campañas activas con nivel de confirmación intermedio-alto.	Medio-Alto
Hashes AlienVault OTX	88 indicadores de archivo provenientes de OTX, asociados a variantes de malware con actividad reciente en Latinoamérica, relevantes para correlación con incidentes en endpoints del sector.	Medio-Alto
Indicadores score 8 fuente única	1.994 indicadores con una sola fuente de validación (Google Threat Intelligence), que representan amenaza confirmada, pero con menor nivel de corroboración independiente. Requieren validación adicional antes de implementar bloqueos masivos.	Medio

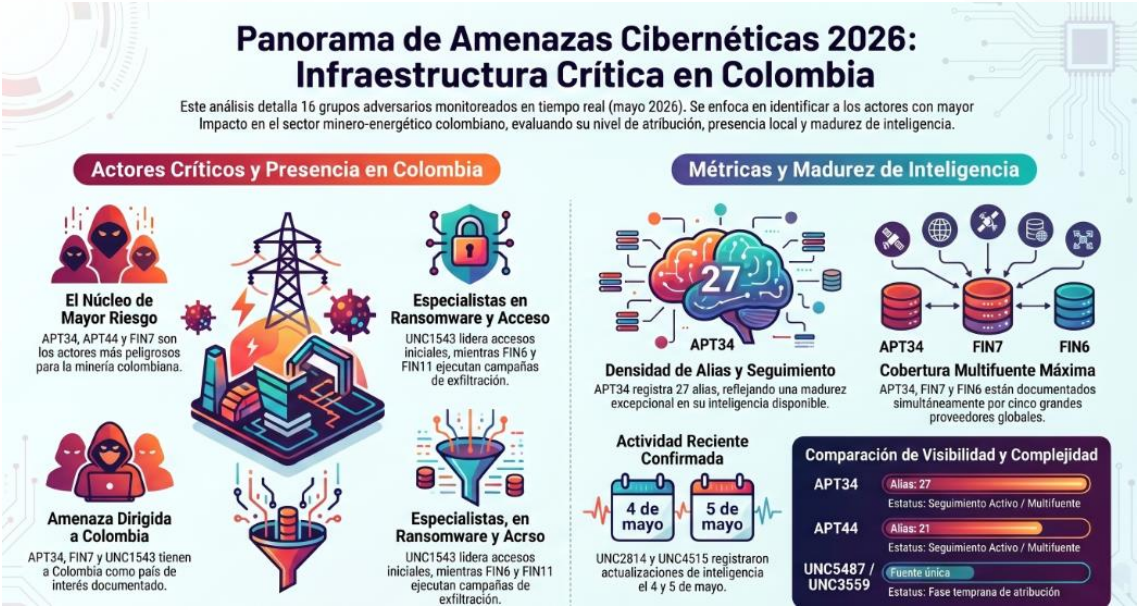
ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Actores Estatales / Espionaje	3	APT44 (Sandworm), APT34, APT19	**Máximo** — Capacidad destructiva sobre infraestructura crítica, espionaje industrial y exfiltración de información estratégica sobre reservas y operaciones mineras
Actores Financieramente Motivados	4	FIN7, FIN6, FIN11, UNC5537	**Alto** — Orientados a extorsión, ransomware y fraude financiero contra empresas del sector con operaciones de alto valor económico
Actores de Acceso Inicial / Distribución	4	UNC1543, UNC3840, UNC2053, UNC5111	**Alto** — Especializados en comprometer entornos corporativos para vender acceso o facilitar campañas de otros actores; presencia documentada en Colombia
Actores de Amenaza Persistente Regional	3	UNC5736, UNC5487, UNC3559	**Medio-Alto** — Actividad confirmada en Latinoamérica con enfoque en sectores de infraestructura y recursos naturales
Actores No Categorizados / En Seguimiento	2	UNC2814, UNC4515	**Medio** — Actividad reciente con actualización en mayo 2026; perfil en construcción con capacidades aún en proceso de atribución formal

Identificación de Actores Relevantes

De los 16 grupos adversarios identificados en el marco de este análisis, tres concentran la mayor atención por su vinculación documentada con Colombia y su historial de operaciones contra sectores de infraestructura crítica, energía e industria extractiva. APT34, APT44 y FIN7 constituyen el núcleo de mayor riesgo para el sector minero colombiano, combinando capacidades técnicas avanzadas, motivaciones alineadas con los activos del sector y actividad reciente confirmada. A estos se suman grupos especializados en acceso inicial como UNC1543, cuya presencia en Colombia está igualmente documentada, y actores financieramente motivados como FIN6 y FIN11, con historial en campañas de ransomware y exfiltración de datos contra empresas de sectores intensivos en activos físicos y digitales. El conjunto de 16 actores confirma que todos se encuentran en seguimiento activo por parte de las fuentes de inteligencia

consultadas, y que sus capacidades y campañas están siendo monitoreadas en tiempo real durante el período de análisis de este informe.



Análisis Cuantitativo de Inteligencia

- **Total, de actores identificados:** 16 grupos adversarios con actividad confirmada, actualizados entre abril y mayo de 2026, todos en seguimiento activo por múltiples proveedores de inteligencia de amenazas a nivel global.

- **Actores con vínculo directo a Colombia:** 3 grupos —APT34, FIN7 y UNC1543— cuentan con Colombia como país de interés documentado dentro de sus perfiles de inteligencia, lo que eleva su nivel de amenaza de genérico a dirigido para el contexto nacional.

- **Densidad de alias por actor:** APT34 registra 27 alias entre proveedores de inteligencia, siendo el actor con mayor número de denominaciones alternativas del conjunto analizado, seguido de APT44 con 21 alias. Esta densidad refleja el nivel de seguimiento global que reciben y la madurez de la inteligencia disponible sobre sus TTPs.

- **Cobertura de fuentes por actor:** Los actores APT34, FIN7 y FIN6 cuentan con la mayor cobertura multifuente, siendo documentados simultáneamente por Google Threat Intelligence, MISP Import, AlienVault OTX Pulse, Malpedia y MITRE ATT&CK Enterprise, lo que proporciona una base sólida para la implementación de controles defensivos basados en TTPs verificados.

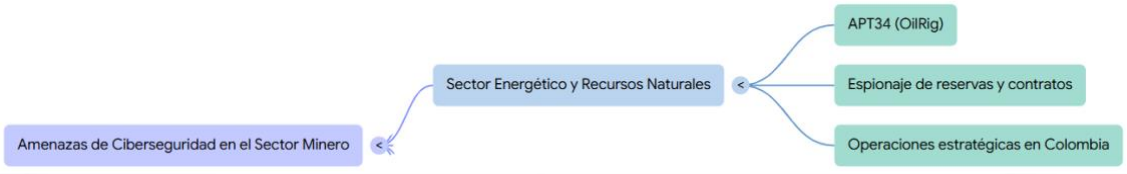
- **Actores con actualización más reciente:** UNC2814 y UNC4515 registran las actualizaciones más recientes del conjunto, con modificaciones el 5 y 4 de mayo de 2026 respectivamente, indicando actividad de inteligencia activa sobre estos grupos en los días inmediatamente anteriores a la publicación de este informe.

- **Actores en etapa de atribución:** UNC5487, UNC3559 y UNC5111 presentan perfiles con fuente única (Google Threat Intelligence), lo que sugiere que se encuentran en fases tempranas de atribución formal, con capacidades identificadas, pero motivaciones y nexos aún en proceso de confirmación por la comunidad de inteligencia.

Objetivos y Sectores Target

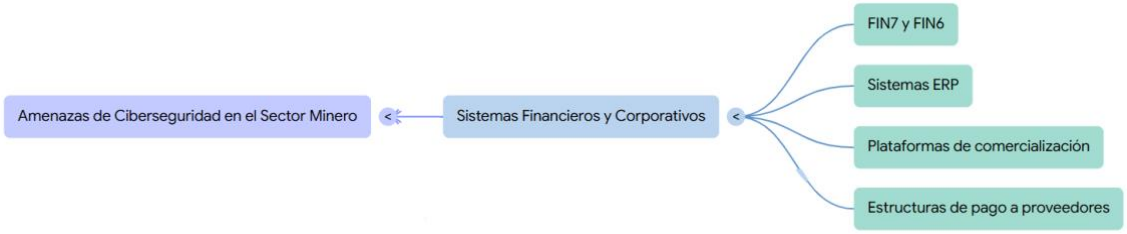
- **Infraestructura crítica industrial (OT/ICS):** APT44 es el actor de mayor amenaza en este dominio, con historial documentado de ataques destructivos contra sistemas de control industrial en sectores minero-energéticos y de servicios. Su presencia en el panorama de amenazas del sector minero colombiano representa el escenario de mayor severidad posible, dado que un ataque exitoso sobre sistemas OT en operaciones mineras puede derivar en interrupciones de producción, daños físicos a equipos y riesgos para la seguridad del personal.

- **Sector Minero-energetico:** APT34, conocido también como OilRig en múltiples fuentes de inteligencia, tiene un historial ampliamente documentado de operaciones contra empresas del sector energético y de extracción en Medio Oriente, con extensión de sus operaciones hacia Latinoamérica. Su perfil de espionaje orientado a información sobre reservas, contratos y operaciones lo posiciona como una amenaza directa para las empresas mineras con activos estratégicos en Colombia.

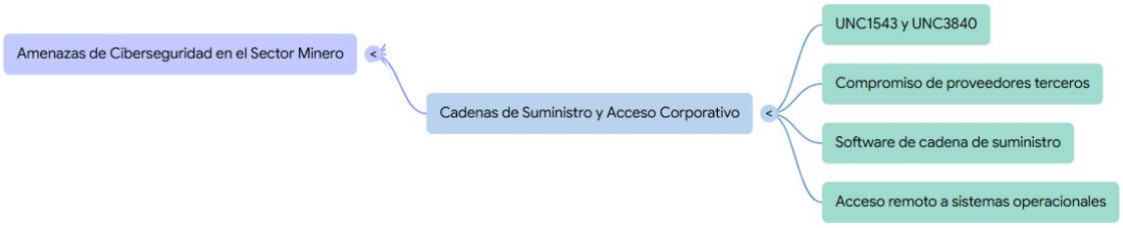


- **Sistemas financieros y corporativos:** FIN7 y FIN6 dirigen sus operaciones principalmente hacia la infraestructura financiera y corporativa de grandes empresas, con énfasis en sistemas de punto de venta, plataformas de gestión financiera y entornos con alta concentración de datos de valor económico. En el

contexto minero, estos actores representan una amenaza directa para los sistemas ERP, plataformas de comercialización de minerales y estructuras de pago a cadena de suministro.

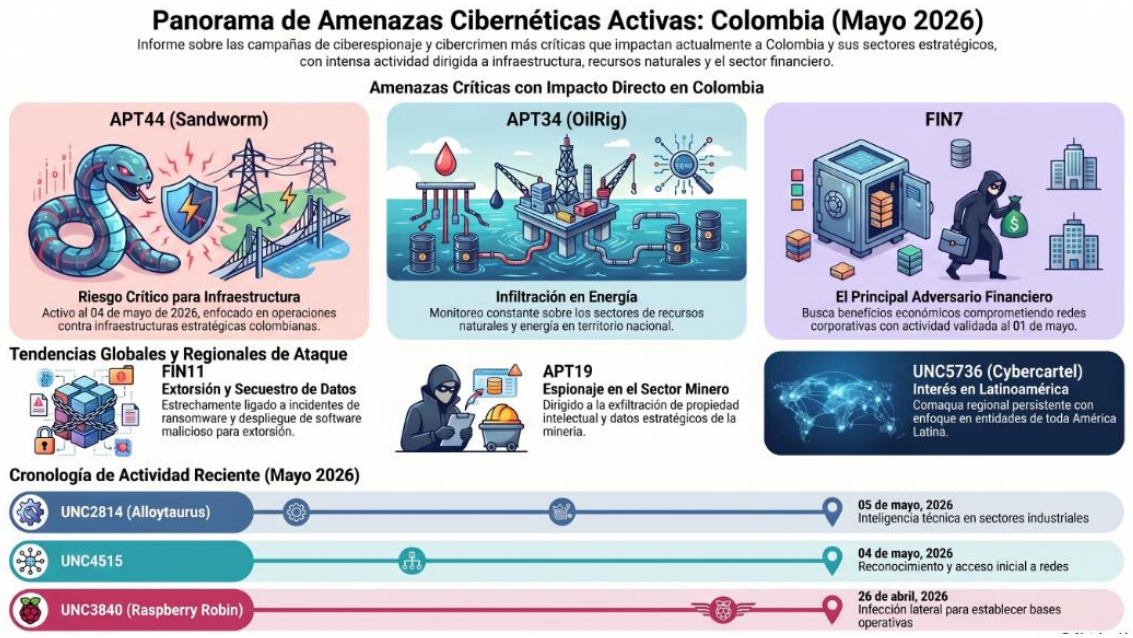


- **Cadenas de suministro y acceso corporativo:** UNC1543 y UNC3840 se especializan en el compromiso de entornos corporativos a través de la cadena de suministro de software y proveedores terceros, un vector de alto riesgo en el sector minero dada la dependencia de contratistas especializados y proveedores de tecnología con acceso remoto a sistemas operacionales.



- **Credenciales y acceso privilegiado:** FIN11 y UNC2053 tienen historial documentado en campañas orientadas al robo de credenciales y el compromiso de cuentas con acceso privilegiado, patrón que guarda coherencia directa con dos de los incidentes más graves del histórico del sector: el compromiso de cuenta con privilegios de mayo 2024 y el acceso no autorizado a información clasificado como Muy Grave en septiembre de 2022.

Campañas Activas



Campañas con Impacto Directo en Colombia

- Campaña APT44 (Sandworm Team): Se mantiene activa con registros recientes al 04 de mayo de 2026. Es una de las amenazas más críticas para el sector debido a su historial de operaciones dirigidas contra infraestructuras estratégicas y su presencia confirmada en territorio colombiano.

- Campaña APT34 (OilRig): Identificada con actividad el 03 de mayo de 2026. Esta campaña se enfoca en la infiltración de sectores de extracción de recursos

naturales y energía, manteniendo un seguimiento constante sobre objetivos en Colombia.

- Campaña FIN7 (Sangria Tempest): Detectada con movimientos al 01 de mayo de 2026. Su objetivo principal es la obtención de beneficios económicos a través del compromiso de redes corporativas, con operaciones validadas en el contexto nacional.

- Campaña UNC1543 (Mustard Tempest): Con actividad registrada el 02 de mayo de 2026, esta campaña ha sido vinculada específicamente con acciones dirigidas hacia organizaciones dentro de Colombia.

Otras Campañas en Curso

- Campaña UNC2814 (Alloytaurus): Es la actividad más reciente registrada (05 de mayo de 2026). Se caracteriza por el espionaje y la recolección de inteligencia técnica en sectores industriales.

- Campaña FIN11 (Lace Tempest): Activa al 03 de mayo de 2026. Esta campaña está estrechamente ligada a incidentes de extorsión y despliegue de software malicioso para el secuestro de información.

- Campaña UNC4515: Identificada con actividad el 04 de mayo de 2026, centrada en la fase de reconocimiento y acceso inicial.

- Campaña FIN6: Con movimientos detectados el 27 de abril de 2026, enfocada en la explotación de activos financieros y datos transaccionales.

- Campaña UNC5736 (Cybercartel): Campaña regional con actividad a finales de abril de 2026, con un interés persistente en entidades de América Latina.

- Campaña UNC3840 (Raspberry Robin): Detectada el 26 de abril de 2026. Utiliza métodos de infección lateral para establecer una base de operaciones dentro de las redes objetivo.

- Campaña APT19 (Deep Panda): Registrada el 24 de abril de 2026, esta campaña de espionaje busca la exfiltración de propiedad intelectual y datos estratégicos del sector minero.

- Campaña UNC5537: Actividad detectada a mediados de abril de 2026, involucrada en la identificación de vulnerabilidades en servicios expuestos.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

Para el informe enfocado en el **sector minero de Colombia**, se ha realizado un mapeo estratégico de las actividades observadas en las campañas activas. Este análisis permite identificar los métodos operativos más probables que los adversarios emplearían para comprometer la infraestructura crítica, el control de procesos y la información estratégica de las organizaciones mineras.

ID	Táctica	Técnica	Justificación para el Sector Minero
TA0001	Acceso Inicial	T1566: Phishing	Método principal utilizado por actores como FIN11 y UNC1543 para obtener acceso inicial a redes corporativas mediante correos dirigidos a personal administrativo o de operaciones.
TA0002	Ejecución	T1059: Command and Scripting Interpreter	Uso de scripts (como Python o PowerShell) para ejecutar comandos maliciosos, común en las fases iniciales de las campañas de APT34.
TA0003	Persistencia	T1133: External Remote Services	Explotación de accesos VPN o escritorios remotos para mantener presencia en la red, técnica habitual de UNC2053 para asegurar acceso continuo a sistemas críticos.
TA0004	Escalada de Privilegios	T1078: Valid Accounts	El uso de credenciales legítimas comprometidas permite a los atacantes moverse con privilegios elevados sin activar alertas inmediatas, observado en campañas de UNC5736.
TA0005	Evasión de Defensas	T1027: Obfuscated Files or Information	Manipulación de archivos para ocultar código malicioso y evadir herramientas de seguridad, una firma operativa constante en los indicadores de APT44.
TA0006	Acceso a Credenciales	T1003: OS Credential Dumping	Extracción de contraseñas directamente de la memoria del sistema para facilitar el movimiento lateral hacia servidores de control industrial o bases de datos.
TA0007	Descubrimiento	T1083: File and Directory Discovery	Búsqueda activa de planos de minas, contratos gubernamentales y datos de prospección, objetivos típicos de espionaje para actores como APT19.
TA0008	Movimiento Lateral	T1210: Exploitation of Remote Services	Aprovechamiento de vulnerabilidades en servicios internos para desplazarse desde la red administrativa hacia la red de control de maquinaria (OT).
TA0009	Recolección	T1119: Automated Collection	Recopilación automática de archivos sensibles para su posterior robo, técnica clave en las campañas de exfiltración de propiedad intelectual.
TA0010	Exfiltración	T1041: Exfiltration Over C2 Channel	Envío de información crítica (financiera o técnica) hacia servidores externos controlados por el atacante, utilizando canales de comunicación ya establecidos.

Cadenas de Ataque Observadas

A continuación, se describen las secuencias lógicas de compromiso detectadas en las actividades de los adversarios analizados para el sector. Estas cadenas representan el flujo de acciones que los atacantes ejecutan para infiltrarse en las redes, escalar privilegios y cumplir sus objetivos de espionaje o beneficio económico en las organizaciones mineras en Colombia.

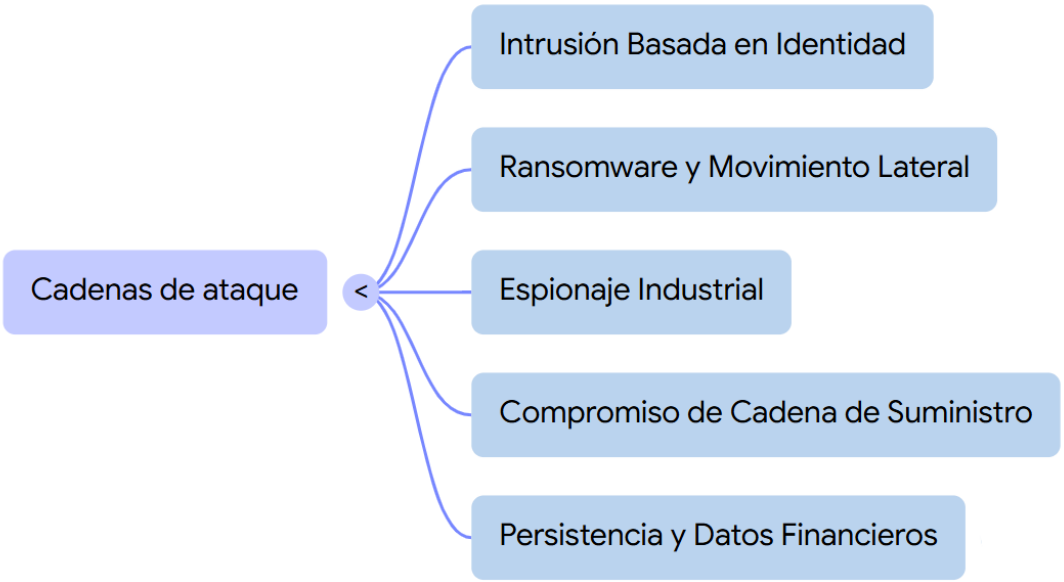
Cadenas de Ataque Observadas

- **Acceso mediante Ingeniería Social** → Ejecución de Scripts Maliciosos → Establecimiento de Persistencia en VPN → Exfiltración de Datos Estratégicos.
- **Explotación de Servicios Remotos Expuestos** → Despliegue de Herramientas de Movimiento Lateral → Acceso a Credenciales de Administrador → Interrupción de Servicios Críticos.
- **Compromiso de Cuentas Válidas** → Reconocimiento de Directorios de Prospección Minera → Recolección Automatizada de Archivos → Envío de Información a Servidores Externos.
- **Infección por Dispositivos Removibles** → Propagación Lateral en la Red Administrativa → Salto a la Red de Control Industrial → Impacto en Procesos Operativos.
- **Distribución de Software Malicioso por Correo** → Evasión de Defensas mediante Ofuscación → Cifrado de Activos Críticos → Demanda de Extorsión Económica.

La comprensión de estas cadenas resulta fundamental para orientar las capacidades defensivas del sector hacia los puntos de intervención más efectivos, priorizando la

detección temprana en las fases iniciales donde el costo de contención es significativamente menor.

Cadenas de ataque:



- **Intrusión Basada en Identidad y Exfiltración de Inteligencia:** Los atacantes utilizan credenciales legítimas comprometidas (técnica observada en grupos como **UNC5736**) para acceder a la red corporativa sin levantar sospechas. Una vez dentro, realizan un reconocimiento exhaustivo de directorios buscando planos de prospección y documentos de concesiones mineras, finalizando con la recolección y envío automatizado de estos activos estratégicos hacia servidores externos.

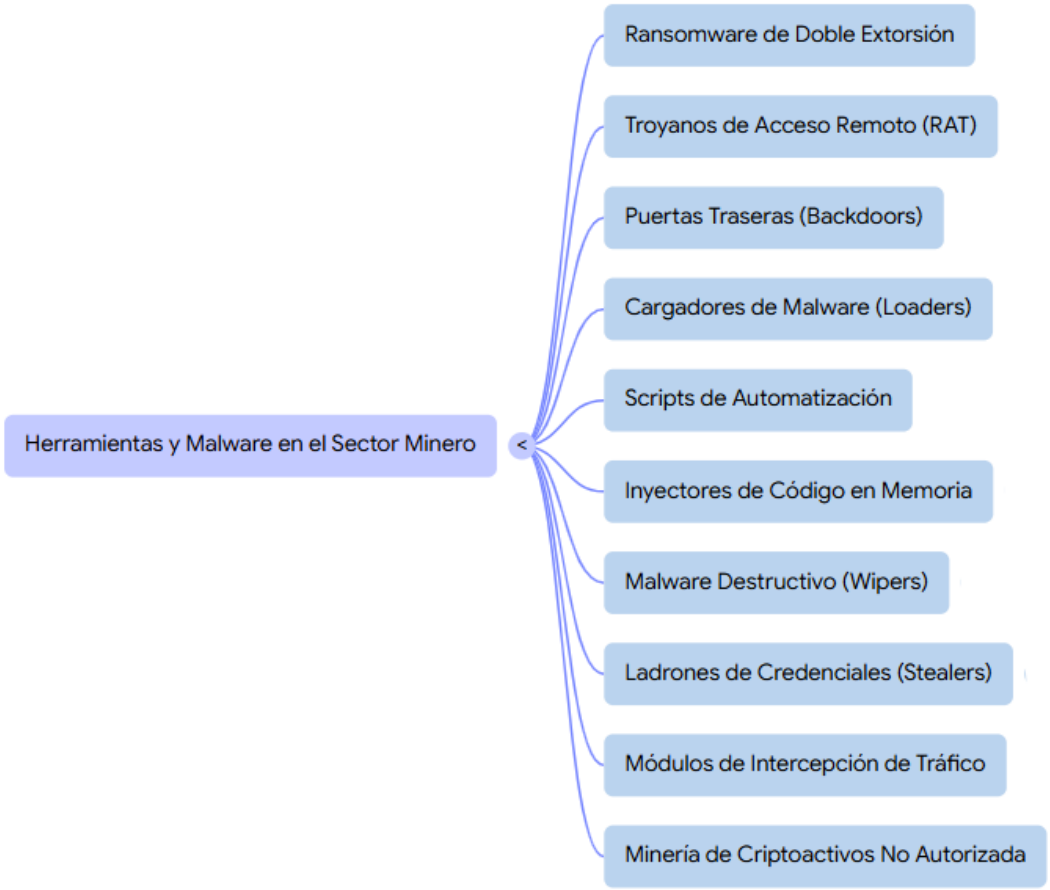
- **Despliegue de Ransomware mediante Movimiento Lateral:** Tras un acceso inicial por servicios remotos como VPNs, el atacante (frecuentemente asociado a campañas como **FIN11**) despliega herramientas para saltar entre servidores internos. El objetivo es alcanzar el controlador de dominio o servidores de respaldo para cifrar la información crítica de la operación minera y exigir un pago por el rescate de los datos.

- **Espionaje Industrial vía Ingeniería Social:** Se inicia con el envío de correos electrónicos dirigidos (Spear-Phishing) a perfiles técnicos o directivos del sector. Al ejecutar el archivo malicioso, se establece una conexión de comando y control (C2) que permite a actores como **APT34** monitorear comunicaciones internas y comunicaciones con el gobierno colombiano para anticiparse a decisiones regulatorias o comerciales.

- **Compromiso de la Cadena de Suministro y Salto a Redes OT:** El atacante compromete a un proveedor de servicios técnicos que tiene acceso a la red de control industrial (OT) de la mina. A través de esta conexión, se introducen scripts que pueden alterar el funcionamiento de maquinaria pesada o sistemas de ventilación, buscando causar una interrupción operativa o daños físicos en la infraestructura.

- **Persistencia Silenciosa para Recolección de Datos Financieros:** Utilizando técnicas de ofuscación de archivos para evadir las defensas tradicionales, grupos como **FIN7** mantienen una presencia prolongada en los sistemas contables. Su cadena se enfoca en interceptar transacciones financieras, desviar pagos a proveedores o recolectar datos bancarios de la organización para su posterior explotación económica.

Herramientas y Malware Específico



- **Ransomware de Doble Extorsión:** Utilizado frecuentemente por grupos como **FIN11**, este tipo de código no solo cifra los archivos críticos de la operación minera (como bases de datos de personal o registros de producción), sino que también exfiltra la información para presionar el pago bajo la amenaza de publicarla.

- **Troyanos de Acceso Remoto (RAT):** Empleados por actores como **APT34** para obtener control total sobre las estaciones de trabajo de ingenieros y geólogos, permitiendo la captura de pantallas, el registro de pulsaciones de teclado y la transferencia de archivos de prospección de manera silenciosa.

- **Puertas Traseras (Backdoors) Personalizadas:** Detectadas en campañas de **APT44**, estas piezas de código se diseñan para evadir sistemas de seguridad tradicionales, permitiendo a los atacantes mantener acceso persistente incluso después de reinicios de sistema o actualizaciones de seguridad.

- **Cargadores de Malware (Loaders):** Como el identificado en la campaña de **UNC3840**, cuya función es descargar y ejecutar módulos adicionales de ataque una vez que el sistema inicial ha sido comprometido, facilitando la propagación lateral dentro de la red corporativa.

- **Scripts de Automatización para Exfiltración:** Basados en lenguajes como Python, estos archivos se encargan de buscar palabras clave relacionadas con "concesiones", "oro", "carbón" o "licitaciones" para empaquetar y enviar la información de interés estratégico hacia servidores externos.

- **Inyectores de Código en Memoria:** Utilizados para ejecutar acciones maliciosas directamente en la memoria RAM del equipo, evitando dejar rastro en el disco duro y dificultando las labores de análisis forense posterior a un incidente.

- **Malware Destructivo (Wipers):** Aunque menos comunes, han sido vinculados a actores de alta intensidad que buscan causar interrupciones operativas totales mediante la eliminación irreversible de sectores de arranque en servidores de control industrial.

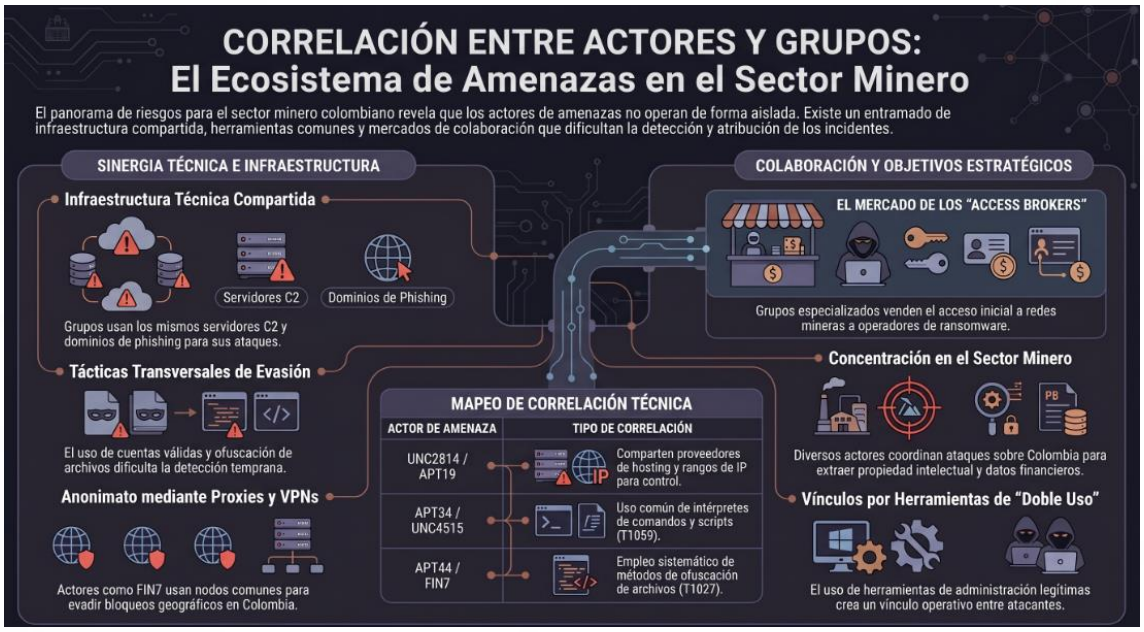
- **Ladrones de Credenciales (Stealers):** Especializados en la extracción de usuarios y contraseñas almacenados en navegadores y aplicaciones de acceso remoto, facilitando el robo de identidad para movimientos laterales rápidos.

- **Módulos de Intercepción de Tráfico:** Componentes que permiten a los atacantes "escuchar" las comunicaciones internas de la red minera, capturando datos sensibles que se transmiten sin el cifrado adecuado entre sedes administrativas y campamentos.

- **Software de Minería de Criptoactivos No Autorizado:** Detectado en infraestructuras con gran capacidad de cómputo, donde los atacantes aprovechan los recursos del servidor para beneficio económico propio, degradando el rendimiento de los sistemas de monitoreo de la mina.

CORRELACIÓN ENTRE ACTORES Y GRUPOS

La identificación de correlaciones entre diversos actores de amenazas permite comprender cómo se entrelazan las capacidades ofensivas en el panorama de riesgos para el sector minero en Colombia. Este análisis revela que muchos grupos no operan de forma aislada, sino que comparten recursos técnicos, infraestructuras de ataque y metodologías operativas, lo que potencia su capacidad de intrusión y dificulta la atribución directa de los incidentes.



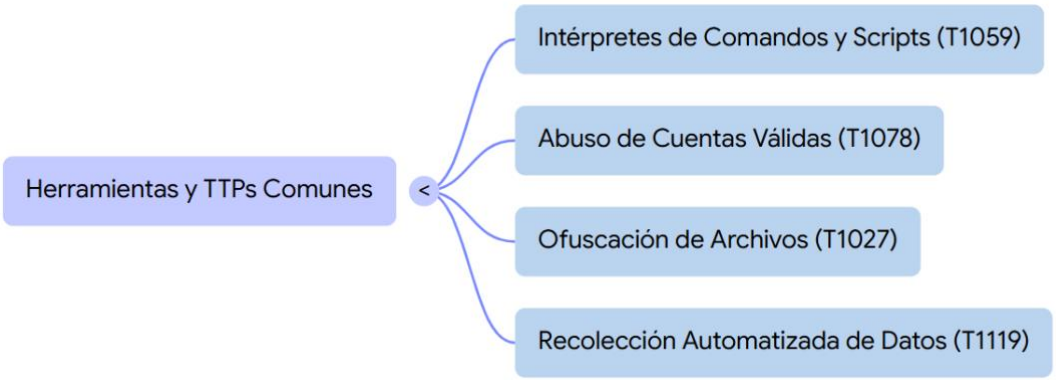
Infraestructura Compartida

- **Servidores de Comando y Control (C2) de Uso Múltiple:** Se ha observado que diferentes campañas, como las de **UNC2814** y **APT19**, utilizan en ocasiones los mismos proveedores de servicios de hosting o rangos de direcciones IP para alojar sus centros de control, facilitando la administración de múltiples infecciones desde un mismo nodo técnico.
- **Dominios de Phishing con Patrones Similares:** Diversos actores emplean servicios de registro de dominios que permiten la creación rápida de sitios web fraudulentos, compartiendo patrones de nomenclatura que imitan servicios legales de correo o portales corporativos del sector minero.
- **Redes de Proxies y VPNs para Anonimato:** El uso de nodos de salida comunes para ocultar el origen real de los ataques es una constante en grupos como **FIN7**

y **FIN6**, quienes aprovechan infraestructuras de red intermedias para evadir bloqueos geográficos en Colombia.

- **Plataformas de Distribución de Cargas Maliciosas:** Actores de menor escala suelen utilizar infraestructuras ya comprometidas por grupos más avanzados para alojar sus propios archivos maliciosos, aprovechando la persistencia establecida previamente en servidores web vulnerables.

Herramientas y TTPs Comunes



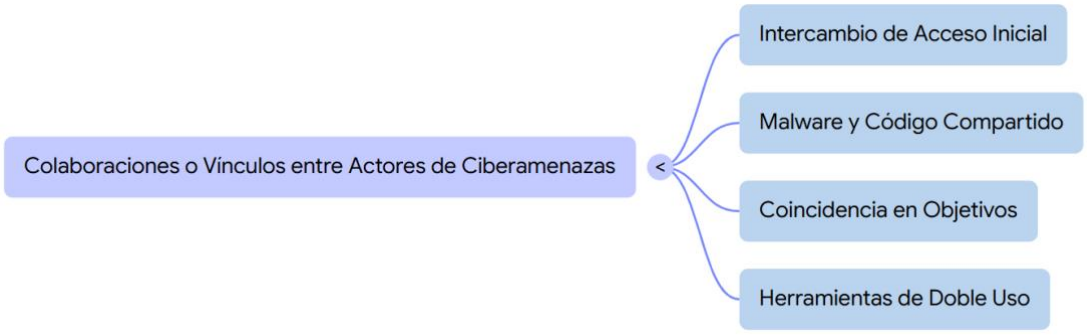
- **Uso de Intérpretes de Comandos y Scripts:** La ejecución de comandos mediante **T1059** es una técnica transversal que permite a grupos como **APT34** y **UNC4515** manipular sistemas sin necesidad de instalar software complejo inicialmente.

- **Abuso de Cuentas Válidas para Persistencia:** Tanto actores financieros como de espionaje coinciden en el uso de **T1078** (Cuentas Válidas) para moverse lateralmente por las redes mineras, aprovechando credenciales filtradas o robadas para pasar desapercibidos ante los sistemas de monitoreo.

- **Métodos de Ofuscación de Archivos:** La técnica **T1027** es empleada de forma sistemática por **APT44** y **FIN7** para ocultar la verdadera naturaleza de sus herramientas, permitiéndoles evadir la detección de soluciones de seguridad que escanean archivos en disco.

- **Recolección Automatizada de Datos:** La implementación de la técnica **T1119** para buscar y empaquetar documentos sensibles es un procedimiento común en campañas que buscan tanto propiedad intelectual como información financiera estratégica.

Posibles Colaboraciones o Vínculos



- **Intercambio de Acceso Inicial (Access Brokers):** Se sospecha que grupos como **UNC3840** (Raspberry Robin) actúan como facilitadores, vendiendo el acceso a redes ya comprometidas a otros actores más especializados, como los grupos de **Ransomware** vinculados a **FIN11**.

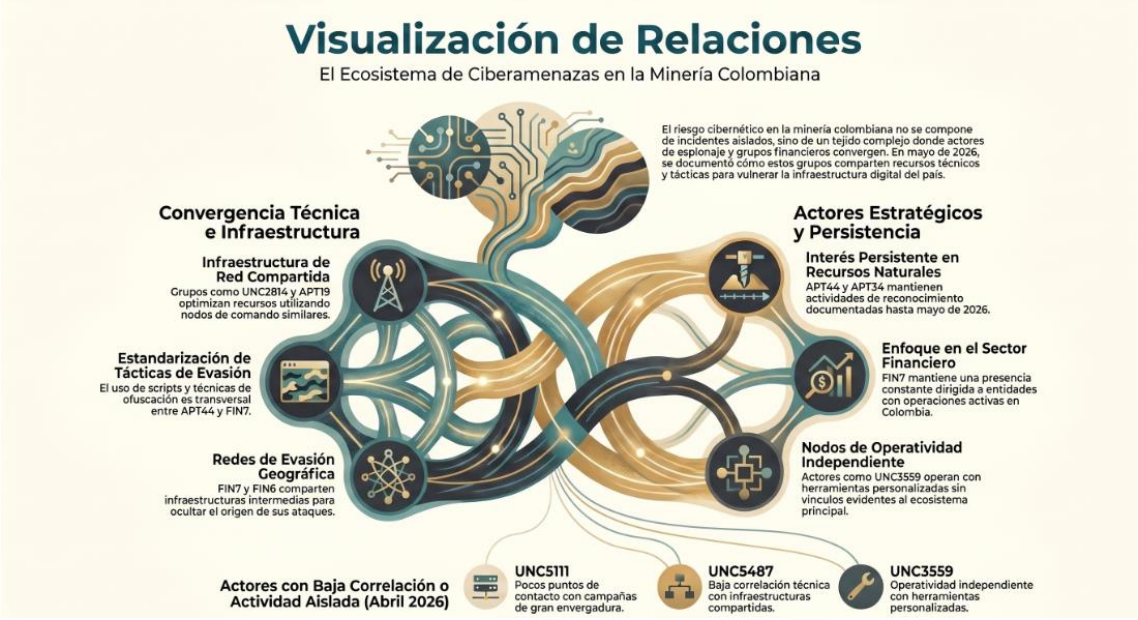
- **Uso de Variantes de Malware Similares:** La similitud en el código base de ciertas herramientas entre **UNC5537** y otros grupos sugiere un posible intercambio de desarrollo o la compra de kits de explotación en foros especializados de la Dark Web.

- **Coincidencia en Objetivos Geográficos y Sectoriales:** La concurrencia de grupos como **APT44**, **APT34** y **UNC1543** con objetivos específicos en **Colombia** durante el mismo periodo de tiempo indica un interés coordinado o competitivo por la información del sector minero nacional.

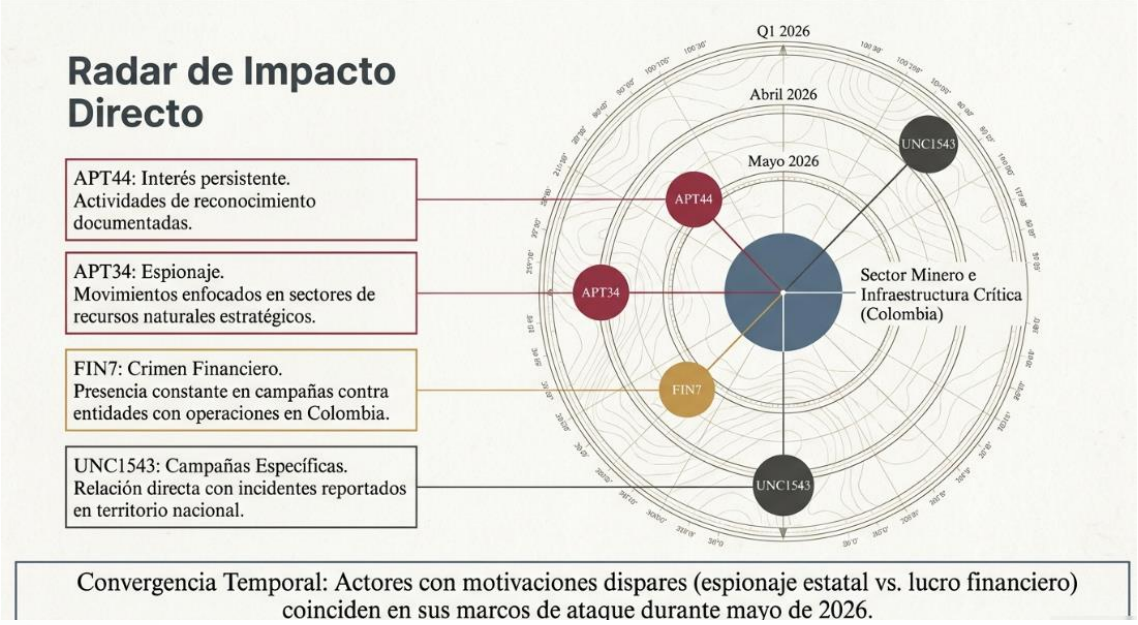
- **Vínculos por Herramientas de "Doble Uso":** El empleo de las mismas herramientas de administración legítimas para fines maliciosos crea un vínculo operativo entre actores que, aunque tengan objetivos diferentes (financieros vs. políticos), utilizan el mismo manual de tácticas para infiltrar organizaciones colombianas.

Visualización de Relaciones

La visualización de relaciones permite comprender el complejo ecosistema de amenazas que gravita sobre el **sector minero en Colombia**. Este análisis identifica cómo diversos actores convergen en puntos críticos de la infraestructura digital y operativa del país, revelando que el riesgo no es una serie de incidentes aislados, sino un tejido de actividades donde grupos con objetivos financieros y de espionaje comparten recursos, tácticas y zonas de influencia.



Relaciones directas documentadas:



Convergencia Temporal: Actores con motivaciones dispares (espionaje estatal vs. lucro financiero) coinciden en sus marcos de ataque durante mayo de 2026.

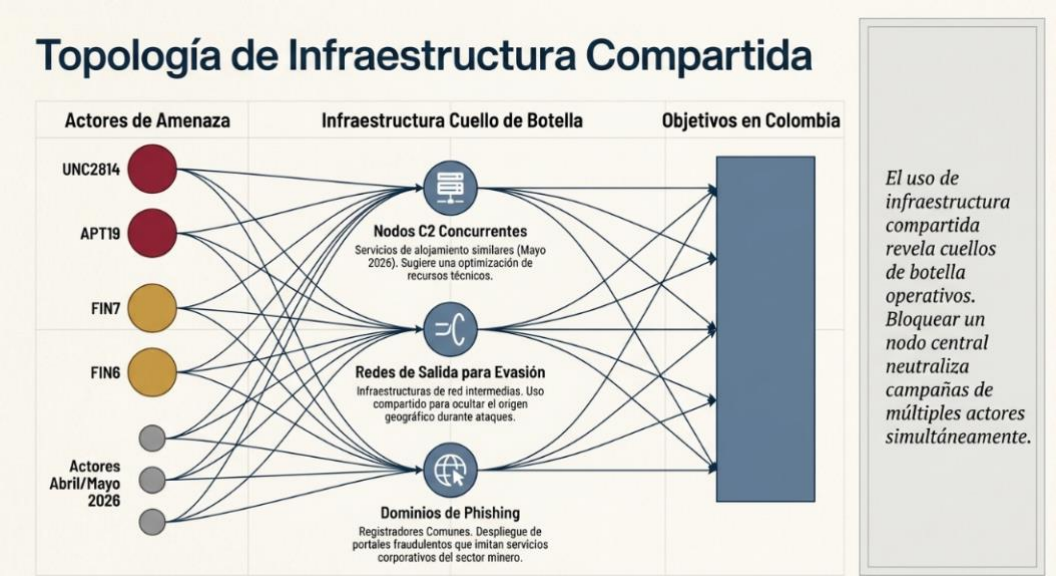
- **Vínculo APT44 y Operaciones en Colombia:** Existe una relación documentada entre este actor y actividades de reconocimiento en el país con registros de mayo de 2026, lo que indica un interés persistente en la infraestructura crítica nacional.

- **Conexión APT34 con Objetivos de Recursos Naturales:** Se han documentado movimientos de este grupo enfocados en sectores estratégicos colombianos, compartiendo marcos temporales de actividad con otros actores de espionaje en mayo de 2026.

- **Relación FIN7 y Sector Financiero Nacional:** Documentado por su presencia constante en campañas dirigidas a entidades con operaciones en Colombia, coincidiendo con reportes de inteligencia de mayo de 2026.

- **Vínculo UNC1543 y Campañas Específicas:** Este actor tiene una relación directa con incidentes reportados en el territorio nacional durante el primer trimestre de 2026.

Relaciones por infraestructura compartida

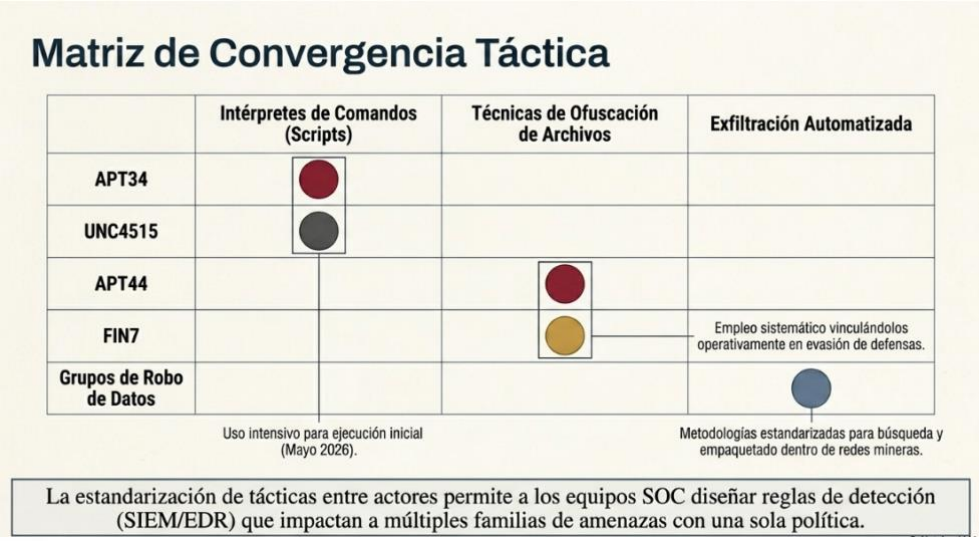


- **Uso de Nodos de Comando y Control (C2) Concurrentes:** Se observa que **UNC2814** y **APT19** han utilizado servicios de alojamiento similares para sus operaciones de mayo de 2026, lo que sugiere una optimización de recursos técnicos.

- **Redes de Salida para Evasión Geográfica:** Grupos como **FIN7** y **FIN6** comparten el uso de infraestructuras de red intermedias para ocultar su origen durante ataques a organizaciones colombianas.

- **Dominios de Phishing en Registradores Comunes:** Diversos actores identificados en abril y mayo de 2026 utilizan los mismos servicios para desplegar portales fraudulentos que imitan servicios corporativos del sector.

Relaciones por herramientas comunes

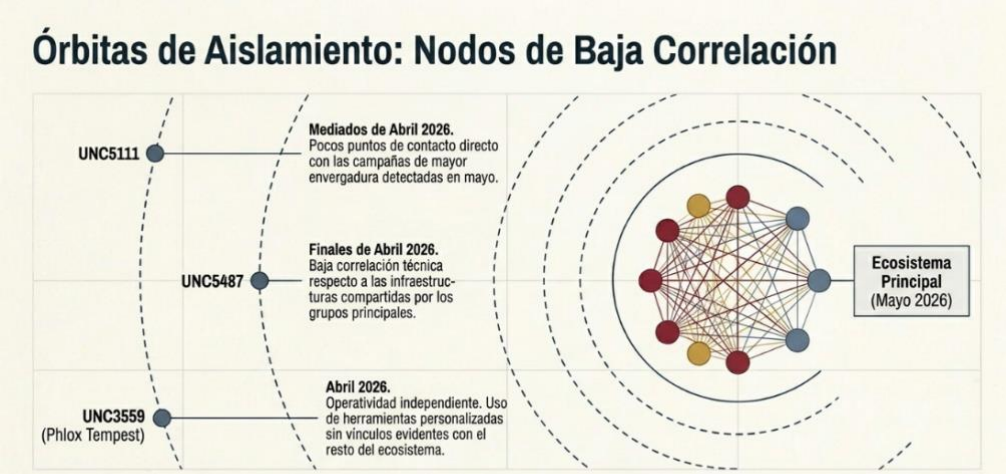


- **Convergencia en el uso de Intérpretes de Comandos:** Actores como **APT34** y **UNC4515** coinciden en el uso intensivo de scripts para la ejecución inicial de sus campañas en mayo de 2026.

- **Adopción Transversal de Técnicas de Ofuscación:** La técnica para ocultar archivos es empleada sistemáticamente tanto por **APT44** como por **FIN7**, vinculándolos operativamente en sus métodos de evasión de defensas.

- **Estandarización de la Exfiltración Automatizada:** Grupos enfocados en el robo de datos estratégicos comparten metodologías para la búsqueda y empaquetado de información sensible dentro de las redes mineras.

Nodos aislados o con baja correlación (por ahora):



La inteligencia de amenazas requiere mapear tanto la convergencia como la divergencia. Estos nodos operan de manera independiente (por ahora), requiriendo perfiles de monitoreo aislados.

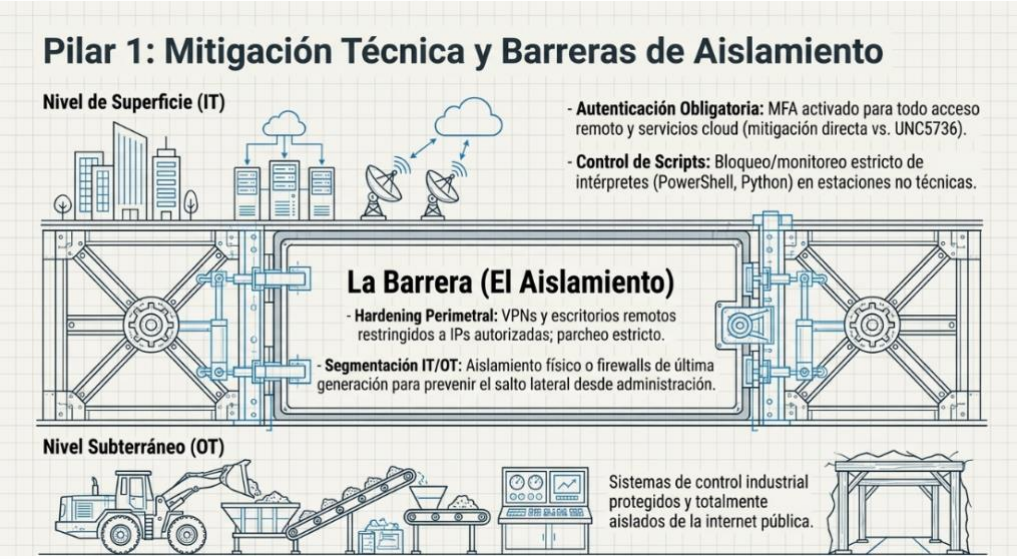
- **UNC5111:** Presenta actividad registrada a mediados de abril de 2026, pero sus métodos y objetivos actuales muestran pocos puntos de contacto directo con las campañas de mayor envergadura detectadas en mayo.
- **UNC5487:** Aunque activo a finales de abril de 2026, se mantiene como un nodo con baja correlación técnica respecto a las infraestructuras compartidas por los grupos principales.
- **UNC3559 (Phlox Tempest):** Sus registros de abril de 2026 indican una operatividad independiente con herramientas personalizadas que no presentan vínculos evidentes con el resto del ecosistema analizado.

RECOMENDACIONES ESTRATÉGICAS

Las recomendaciones estratégicas para el **sector minero en Colombia** se fundamentan en la necesidad de proteger tanto la propiedad intelectual (prospección y licitaciones) como la continuidad de la operación física en los campamentos. Dado el perfil de los actores identificados, que combinan el espionaje estatal con la extorsión financiera, la estrategia debe ser integral, cubriendo desde el blindaje de la identidad digital hasta la capacidad de respuesta ante interrupciones en los sistemas de control industrial.

Recomendaciones de Mitigación Técnica

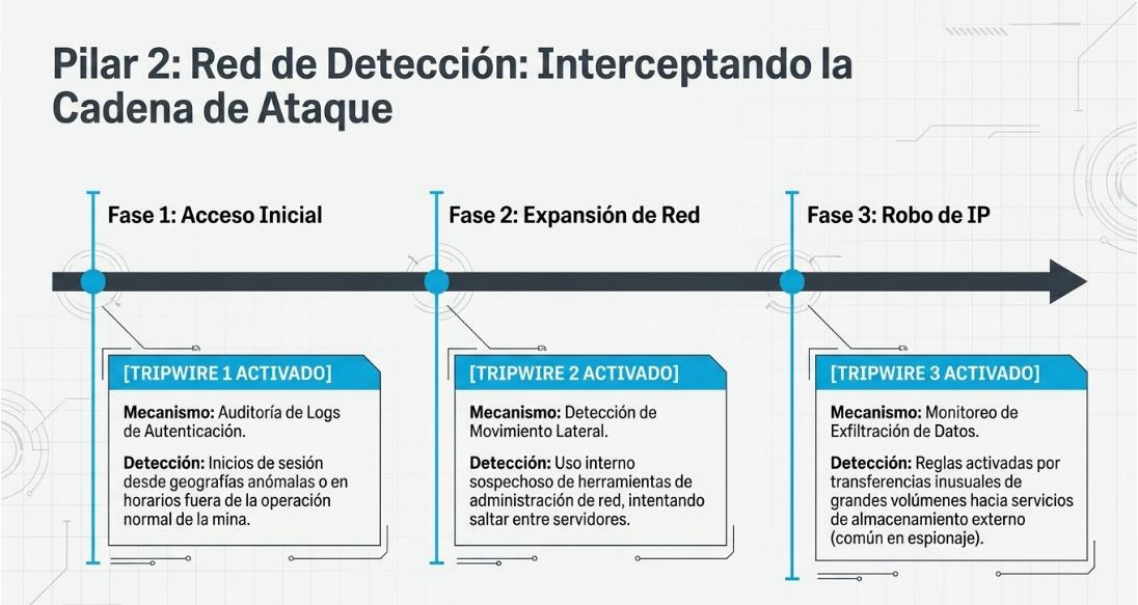
Para reducir la superficie de exposición frente a las tácticas de acceso inicial y ejecución observadas en las campañas activas, se sugieren las siguientes medidas:



- **Implementación de Autenticación Multifactor (MFA):** Establecer MFA de manera obligatoria para todos los accesos remotos y servicios en la nube, mitigando el uso de cuentas válidas robadas por grupos como **UNC5736**.
- **Segmentación de Redes (IT/OT):** Aislar físicamente o mediante firewalls de última generación la red administrativa de los sistemas de control de maquinaria minera para prevenir movimientos laterales.
- **Hardening de Servicios Remotos:** Restringir el acceso a VPNs y escritorios remotos únicamente a direcciones IP autorizadas y mantener los parches de seguridad al día para evitar la explotación de servicios expuestos.
- **Control de Ejecución de Scripts:** Bloquear o monitorear estrictamente el uso de intérpretes de comandos como PowerShell o Python en estaciones de trabajo no técnicas para frenar la ejecución de malware inicial.

Recomendaciones de Detección y Monitoreo

Es fundamental fortalecer las capacidades de visibilidad para identificar comportamientos anómalos antes de que se complete la cadena de ataque:



- **Monitoreo de Exfiltración de Datos:** Implementar reglas de detección para transferencias inusuales de grandes volúmenes de datos hacia servicios de almacenamiento externo, comunes en tácticas de espionaje.
- **Auditoría de Logs de Autenticación:** Establecer alertas ante inicios de sesión desde ubicaciones geográficas no habituales o en horarios fuera de la operación normal de la mina.
- **Detección de Movimiento Lateral:** Supervisar el uso interno de herramientas de administración de red para identificar atacantes intentando saltar entre servidores.

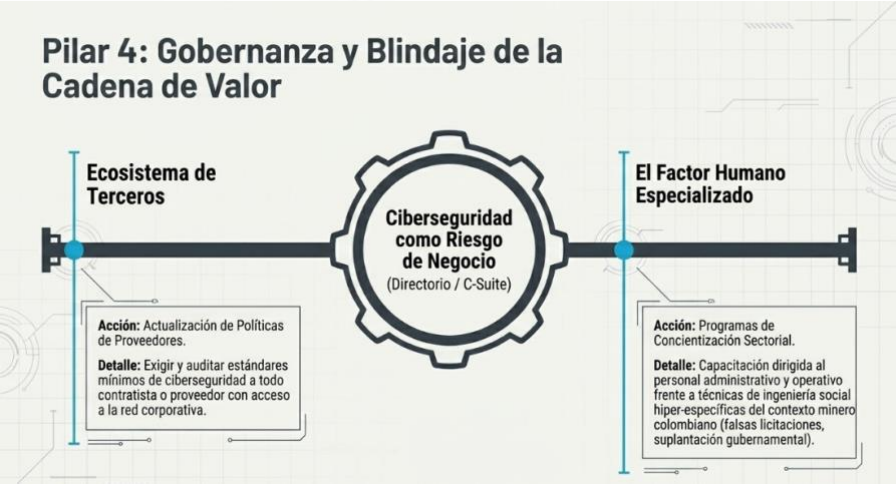
Recomendaciones de Resiliencia Operativa

La capacidad de mantener la producción minera a pesar de un compromiso digital es vital para la estabilidad financiera de la organización:

- **Estrategia de Respaldos Off-site:** Mantener copias de seguridad de los datos críticos fuera de la red principal y desconectadas (Air-gapped) para garantizar la recuperación ante ataques de ransomware de grupos como **FIN11**.
- **Redundancia de Sistemas Críticos:** Asegurar que los sistemas de seguridad física y ventilación en mina tengan modos de operación manual o redundancia digital aislada.

Recomendaciones de Gobernanza

La seguridad debe ser tratada como un riesgo de negocio y no solo como un problema técnico del departamento de sistemas:



- **Actualización de Políticas de Terceros:** Exigir estándares mínimos de ciberseguridad a los contratistas y proveedores que tienen acceso a la red de la compañía.
- **Programas de Concientización Sectorial:** Capacitar al personal administrativo y operativo sobre los riesgos de ingeniería social específicos para el contexto minero colombiano.

Preparación ante Incidentes

Estar listos para actuar de forma coordinada reduce significativamente el impacto reputacional y económico:

- **Simulacros de Respuesta a Incidentes:** Realizar ejercicios de mesa (Tabletop) basados en los escenarios de ataque descritos, involucrando a la alta gerencia y equipos legales.
- **Canales de Comunicación de Emergencia:** Definir medios de comunicación alternos para la coordinación del equipo de crisis en caso de que la red interna sea comprometida.

Acciones Inmediatas (Quick Wins)

Pasos rápidos que pueden ejecutarse en el corto plazo para elevar el nivel de protección de manera inmediata:

Síntesis: Hoja de Ruta Ejecutiva de Implementación

Iniciativa	Pilar de Defensa	Esfuerzo	Foco de Mitigación	Responsable Sugerido
Revocación Privilegios, Carga IoC (.xlsx), Cierre Puertos	Quick Wins	Bajo	Acceso Inicial	TI / Seguridad Corporativa
MFA Obligatorio, Bloqueo PowerShell	Mitigación	Medio	Espionaje Estatal	TI
Segmentación IT/OT, Hardening VPN	Mitigación	Alto	Extorsión / OT	TI & OT
Reglas Exfiltración, Alertas Logs & Movimiento Lateral	Detección	Medio	Espionaje y Expansión	Operaciones de Seguridad (SOC)
Backups Air-Gapped, Redundancia Manual (Ventilación)	Resiliencia	Alto	Extorsión (Ransomware)	TI & Gerencia de Mina
Auditoría Contratistas, Concientización	Gobernanza	Medio	Acceso Inicial	Legal, RRHH, TI
Tabletops, Comms Out-of-Band	Preparación	Bajo	Impacto Reputacional	Alta Gerencia y Legal

El plano digital requiere ejecución coordinada entre las divisiones de Tecnología (IT), Operación Minera (OT) y el Directorio Ejecutivo.

- **Revisión de Privilegios de Administrador:** Eliminar permisos elevados de cuentas que no los requieran estrictamente para sus funciones diarias.
- **Cierre de Puertos No Críticos:** Realizar un escaneo externo rápido y cerrar cualquier servicio que no sea esencial para la operación y que esté expuesto a Internet.

CONCLUSIONES

1. Amenaza Dirigida y No Incidental

El sector minero en Colombia no enfrenta una exposición genérica, sino una **amenaza dirigida**. La identificación de grupos como **APT34, FIN7 y UNC1543**, que tienen a Colombia explícitamente documentado como país de interés, confirma que los activos minerales estratégicos (litio, cobre, oro) posicionan al país como un blanco deliberado para el ciberespionaje estatal y la extorsión financiera.

2. Infraestructura Maliciosa en Estado Crítico y Activo

La inteligencia técnica revela un ecosistema de ataque vigente y de alta peligrosidad. Con **3.347 indicadores de compromiso (IoCs) activos** y una ventana de expiración proyectada entre mayo y julio de 2026, el riesgo es inmediato. La alta concentración

de indicadores de severidad en direcciones IP sugiere la existencia de servidores de comando y control (C2) operando en tiempo real contra la infraestructura nacional.

3. Vulnerabilidad Crítica en la Convergencia TI/OT
La transformación digital del sector ha creado una superficie de ataque híbrida donde la interconexión entre las redes administrativas (TI) y los **Sistemas de Control Industrial (OT/SCADA)** representa el mayor riesgo operativo. Actores con capacidades destructivas, como **APT44 (Sandworm)**, tienen el potencial de saltar de sistemas corporativos a redes de control, pudiendo causar daños físicos en maquinaria, interrupciones de ventilación en minas y riesgos para la vida del personal.

4. El Phishing como Vector de Entrada Dominante
A pesar de la sofisticación técnica de los grupos, el **factor humano** sigue siendo el eslabón más explotado. El fraude y la suplantación representan el 47% de los incidentes históricos del sector. La presencia masiva de dominios que imitan servicios legítimos (Microsoft, Adobe, servicios cloud) confirma que la ingeniería social dirigida a empleados y contratistas es la técnica de acceso inicial preferida por los adversarios.

5. Centralización del Riesgo y Efecto Cascada en la Cadena de Suministro
Existe una alta concentración de incidentes en **Bogotá D.C. (91%)**, debido a la centralización de los sistemas de gestión y plataformas de gobierno. Sin embargo, el riesgo se extiende mediante la **cadena de suministro**, donde el compromiso de un contratista o proveedor con acceso remoto a la mina actúa como un "caballo de Troya" para infiltrar las operaciones en zonas remotas.

6. Necesidad de una Ciberdefensa Proactiva y Soberana
Dada la sofisticación de los actores identificados, muchos de ellos con vínculos a servicios de inteligencia extranjeros, la ciberseguridad del sector debe trascender lo técnico para convertirse en un pilar de **soberanía nacional**. Una postura reactiva es insuficiente; se requiere una estrategia basada en la inteligencia de amenazas, el monitoreo constante de IoCs y la resiliencia operativa que garantice que, incluso ante un compromiso digital, la producción física de la mina no se detenga.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **Ataque de Denegación de Servicio (DoS/DDoS):** Intento deliberado de interrumpir el tráfico normal de un servidor, servicio o red inundando la infraestructura con tráfico de internet.
- **Ciberespionaje:** Uso de ataques informáticos para obtener información confidencial de gobiernos o competidores con fines estratégicos o económicos.
- **Grupo de Amenaza (Actor de Amenaza):** Conjunto de individuos u organizaciones con la intención y capacidad de realizar actividades maliciosas (ej: APT34, Sandworm).
- **Indicadores de Compromiso (IoCs):** Evidencias forenses (como IPs, hashes o dominios) que indican que un sistema ha sido vulnerado.
- **Ingeniería Social:** Táctica de manipulación psicológica que busca que los usuarios revelen información confidencial o realicen acciones como descargar malware.
- **Severidad (Criticality):** Nivel de peligro asignado a una amenaza o vulnerabilidad; en el sector minero, la mayoría de los indicadores registrados son de severidad "Alta" o "Crítica".

Infraestructura y Redes

- **C2 (Comando y Control):** Infraestructura de servidores utilizada por los atacantes para enviar instrucciones a sistemas comprometidos y extraer datos.
- **Convergencia TI/OT:** Integración de los sistemas de Tecnologías de la Información (oficinas) con las Tecnologías de Operación (maquinaria de mina, sensores).
- **Dominio Malicioso:** Nombre de sitio web registrado o utilizado por atacantes para distribuir malware o realizar campañas de phishing.
- **IP (Dirección IP):** Etiqueta numérica que identifica un dispositivo en una red. El informe destaca que las direcciones IP son el tipo de indicador más frecuente en los ataques actuales.

- **SCADA:** Sistemas de control y adquisición de datos que permiten supervisar y controlar procesos industriales a distancia, críticos en la operación minera.

Herramientas y Malware

- **Exploit:** Fragmento de software o secuencia de comandos que aprovecha una vulnerabilidad para causar un comportamiento no deseado en un sistema.
- **Malware:** Software diseñado con intenciones maliciosas, que incluye virus, troyanos y programas espía.
- **Phishing:** Método de engaño mediante correos electrónicos o mensajes falsos para robar credenciales; representa el 47% de los incidentes en el sector.
- **Ransomware:** Tipo de malware que cifra la información del usuario y exige un rescate económico para su liberación.
- **Troyano (Trojan):** Malware que se presenta como una herramienta legítima para engañar al usuario y permitir el acceso remoto del atacante.

Sector

- **Cadena de Suministro (Supply Chain):** Conjunto de proveedores y contratistas. El riesgo de suministro es crítico en minería debido a la dependencia de terceros para el mantenimiento de maquinaria.
- **Infraestructura Crítica:** Sistemas y activos tan vitales que su incapacidad o destrucción tendría un impacto debilitante en la seguridad o economía nacional.
- **MISP (Malware Information Sharing Platform):** Plataforma de código abierto para compartir, almacenar y correlacionar indicadores de compromiso entre organizaciones.
- **Resiliencia Operativa:** Capacidad de una organización para mantener sus funciones esenciales durante y después de un ciberataque.

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