TIC

Informe de apreciación Sector

Industria

COLCERT

Contenido

Informe de apreciación
Sector Industria

COLCERT IN-20260629-033

TLP: CLEAR

RESUMEN EJECUTIVO

En el sector industria de Colombia, la acelerada adopción de tecnologías de automatización y la profunda integración entre las redes corporativas y los sistemas de control de procesos han expandido significativamente la superficie de exposición ante ciberamenazas. Actores con capacidades técnicas avanzadas, especialistas en intrusión y operadores de software extorsivo dirigen sus acciones hacia infraestructuras de manufactura y producción, buscando comprometer la continuidad operativa, la propiedad intelectual y la estabilidad económica de los activos estratégicos del país.

Este informe emplea inteligencia de amenazas estratégica para realizar un seguimiento detallado al comportamiento de los adversarios que impactan el sector industrial, a partir de la correlación de datos técnicos y operativos analizados. Se priorizan fuentes de visibilidad global y nacional que aportan datos accionables sobre amenazas vigentes, permitiendo que las organizaciones industriales transiten de una postura defensiva reactiva hacia una gestión de riesgos informada y proactiva.

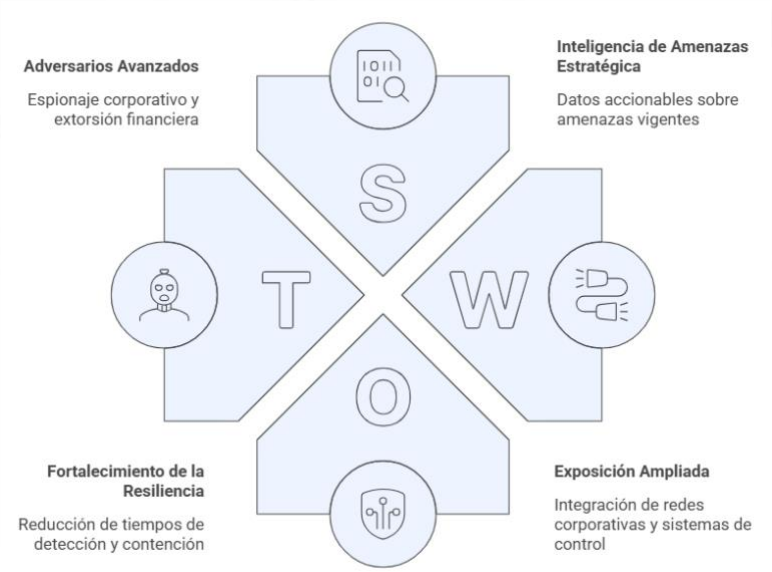
Lineamientos

- Seguimiento y perfilamiento de actores que afectan el sector industria en Colombia.
- Uso de inteligencia de amenazas para la identificación de patrones de ataque y persistencia.
- Priorización de fuentes de ciberinteligencia aplicables al contexto de la infraestructura productiva nacional.
- Enfoque en la protección de sistemas de gestión de activos y procesos industriales estratégicos.
- Reducción de tiempos de detección y contención ante incidentes de alta severidad operativa.
- Fortalecimiento de la resiliencia cibernética para garantizar la disponibilidad de las líneas de producción y la integridad de los datos industriales.

Informe de apreciación
Sector Industria

COLCERT IN-20260629-033

TLP: CLEAR



INTRODUCCIÓN

El sector industrial en Colombia enfrenta un panorama de riesgo híbrido, donde convergen motivaciones de espionaje corporativo y extorsión financiera. La presencia de actores con capacidades avanzadas sugiere un interés persistente en la interrupción de procesos productivos y el robo de propiedad intelectual. La integración de tecnologías operativas con redes corporativas ha ampliado la superficie de exposición, permitiendo que adversarios con historial de ataques a infraestructuras críticas mantengan operaciones activas en la región.

Aspectos clave

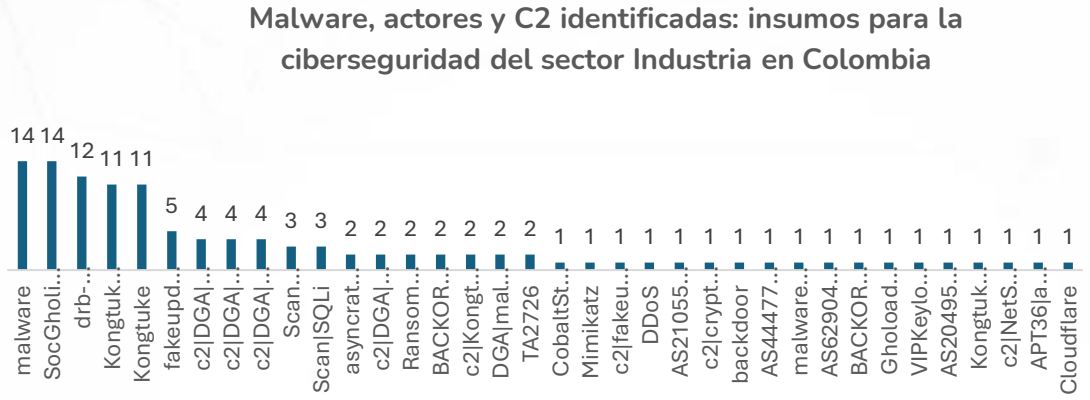
- Persistencia de adversarios especializados en el sector energético e industrial.
- Predominio de campañas de obtención de credenciales y acceso inicial.
- Riesgo elevado de despliegue de software malicioso con fines de extorsión.
- Enfoque geográfico específico en activos estratégicos colombianos.
- Convergencia de amenazas que afectan tanto la continuidad de negocio como la integridad de los datos.

Informe de apreciación
Sector Industria

COLCERT IN-20260629-033

TLP: CLEAR

Hallazgos Clave



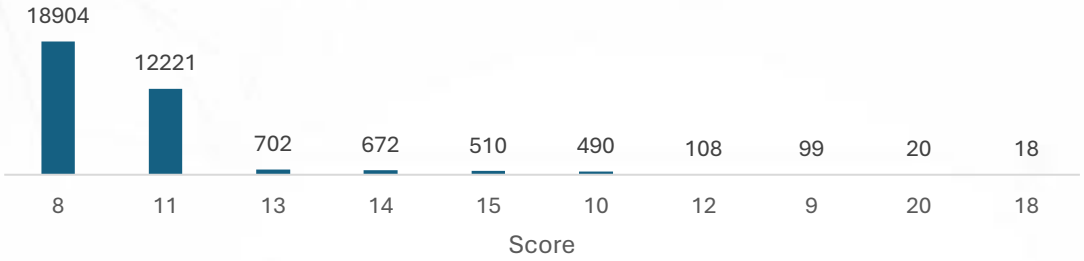
- **Actividad Adversaria de Alto Nivel:** Se identifica la presencia de grupos con historial de sabotaje industrial y ataques a redes eléctricas, los cuales han adaptado sus tácticas para infiltrarse en organizaciones nacionales.

- **Explotación de Cadena de Suministro:** Los adversarios están aprovechando debilidades en proveedores de servicios y software para ganar acceso lateral a las redes industriales principales.

- **Evolución del Fraude Financiero:** Se observa una sofisticación en los métodos de movimiento lateral dentro de redes corporativas del sector industrial para facilitar transferencias no autorizadas y secuestro de información sensible.

- **Interés Geopolítico y Económico:** La recurrencia de ciertos grupos sugiere que Colombia es un objetivo estratégico para el monitoreo de recursos naturales y procesos de manufactura a gran escala.

Score de riesgo por etiqueta (8–20) — Sector Industria de Colombia



Recomendaciones Prioritarias

- **Segmentación Estricta de Redes:** Implementar una separación física o lógica rigurosa entre los entornos de control de procesos industriales y las redes administrativas para prevenir el movimiento lateral de amenazas.
- **Fortalecimiento de la Identidad:** Establecer protocolos de autenticación robustos y revisiones periódicas de privilegios, especialmente para accesos remotos de terceros y contratistas.
- **Monitoreo de Anomalías en Tiempo Real:** Desarrollar capacidades para detectar comportamientos inusuales en el tráfico de red y en la ejecución de procesos que no correspondan a la operación normal de la planta.
- **Programas de Respuesta a Incidentes Especializados:** Diseñar y probar planes de recuperación que consideren la restauración de sistemas críticos industriales, minimizando el impacto en la producción física.

Conclusión Estratégica

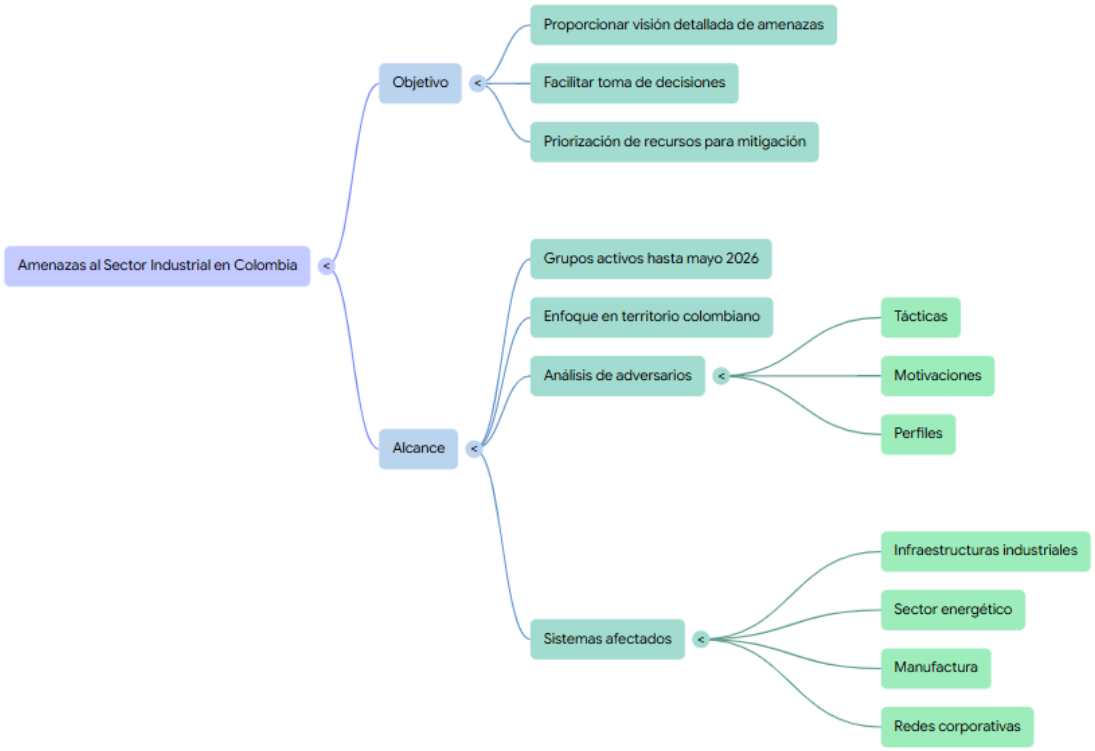
La estabilidad operativa del sector industrial colombiano depende de la transición de una postura de defensa reactiva a una proactiva. Dada la naturaleza de los adversarios identificados, que poseen capacidades para el impacto persistente y el sabotaje, la ciberseguridad debe ser tratada como un componente crítico de la continuidad de la producción. La resiliencia no solo requiere protección tecnológica, sino una alineación estratégica que proteja los activos físicos a través de la seguridad digital.

Informe de apreciación
Sector Industria

COLCERT IN-20260629-033

TLP: CLEAR

OBJETIVO Y ALCANCE



Objetivo

El presente informe tiene como finalidad proporcionar una visión clara y detallada sobre las amenazas que impactan directamente al sector industrial en Colombia. Se busca facilitar la toma de decisiones informada para los niveles ejecutivos y tácticos, permitiendo la priorización de recursos hacia la mitigación de los riesgos con mayor probabilidad de ocurrencia e impacto.

Alcance

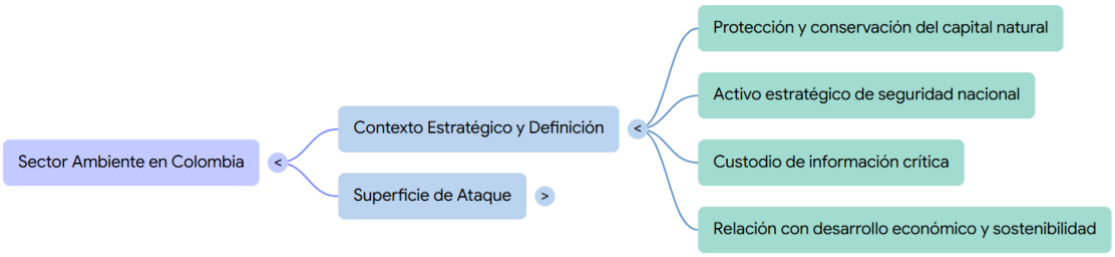
El análisis comprende la evaluación de grupos de amenazas activos detectados hasta mayo de 2026, con un enfoque particular en su comportamiento dentro del territorio colombiano. El informe se limita al análisis de tácticas, motivaciones y perfiles de adversarios que han demostrado interés o actividad en infraestructuras industriales, energéticas y de manufactura, así como en las redes corporativas que las sustentan.

Este informe abarca:

- Identificación de perfiles de adversarios con actividad regional.

- Análisis de motivaciones (espionaje, financiero, sabotaje).
- Evaluación de la persistencia de las amenazas en Colombia.
- Determinación de riesgos para la continuidad operativa industrial.

CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR

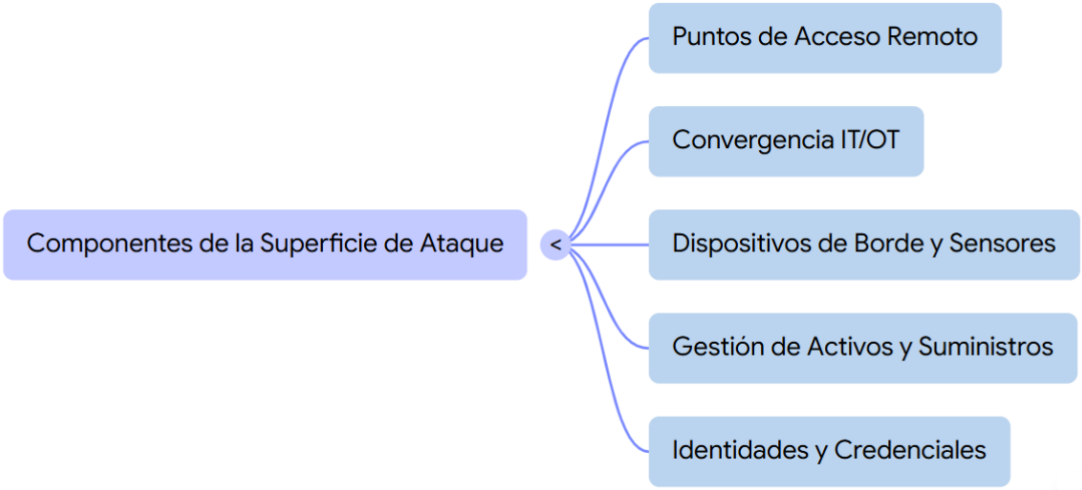


Definición y Entendimiento del Sector

El sector industrial en Colombia constituye uno de los pilares fundamentales de la economía nacional, abarcando desde la manufactura de bienes de consumo hasta el procesamiento de recursos naturales y la producción de energía. Este sector se caracteriza por una creciente dependencia de la automatización y la digitalización, donde la convergencia entre los sistemas de gestión empresarial y los sistemas de control de procesos físicos es cada vez más profunda. Esta interconexión, si bien optimiza la eficiencia y la productividad, introduce desafíos de seguridad únicos, ya que los activos industriales no solo deben proteger la confidencialidad de la información, sino, primordialmente, garantizar la integridad de los procesos y la disponibilidad continua de las líneas de producción para evitar impactos económicos y sociales a gran escala.

Superficie de Ataque

La superficie de ataque en el entorno industrial colombiano se ha expandido significativamente debido a la modernización de las infraestructuras y la adopción de modelos de trabajo remoto para supervisión técnica. Los vectores de entrada ya no se limitan al perímetro físico de la planta, sino que se extienden a través de diversos canales digitales que conectan la operación interna con el mundo exterior.



Componentes clave de la superficie de ataque:

- **Puntos de Acceso Remoto:** La utilización de conexiones para mantenimiento técnico y gestión de proveedores externos crea puertas de entrada que, de no estar debidamente protegidas, permiten a los adversarios infiltrarse en el núcleo de la operación.

- **Convergencia IT/OT:** La eliminación del aislamiento tradicional entre las redes administrativas y las redes de producción permite que una amenaza iniciada en un correo electrónico corporativo pueda escalar hasta detener una turbina o una línea de ensamblaje.

- **Dispositivos de Borde y Sensores Inteligentes:** La proliferación de dispositivos conectados que monitorean variables físicas aumenta los puntos finales que deben ser gestionados, muchos de los cuales carecen de capacidades nativas de defensa avanzada.

- **Sistemas de Gestión de Activos y Suministros:** Las plataformas digitales que gestionan la logística y el inventario representan un objetivo crítico, ya que su alteración puede paralizar la cadena de suministro nacional e internacional.

- **Identidades y Credenciales de Operadores:** El factor humano sigue siendo un eslabón vulnerable; el compromiso de las credenciales de un supervisor de planta puede otorgar a un atacante el control total sobre procesos críticos sin necesidad de explotar vulnerabilidades técnicas complejas.

Informe de apreciación
Sector Industria

COLCERT IN-20260629-033

TLP: CLEAR

PANORAMA ACTUAL DE AMENAZAS

A mayo de 2026, el sector industrial en Colombia se consolida como el objetivo principal de ataques cibernéticos, concentrando el mayor volumen de incidentes reportados en el país por encima del sector financiero y comercial. El panorama actual está marcado por una sofisticación sin precedentes en las técnicas de acceso, donde los adversarios han integrado capacidades de automatización avanzada para identificar y explotar vulnerabilidades en cuestión de horas tras su descubrimiento. Se observa una transición crítica desde ataques genéricos hacia operaciones de precisión que utilizan identidades comprometidas y técnicas de suplantación de alta fidelidad, permitiendo a los atacantes evadir los controles perimetrales tradicionales. La tendencia dominante refleja un ecosistema donde la extorsión mediante el secuestro de información operativa y la exfiltración de propiedad intelectual son los principales motores, afectando la estabilidad de las cadenas de suministro y la continuidad de la producción nacional.

TITULO	FECHA	FUENTE / ENLACE
Gestión de incidentes de ciberseguridad en el sector público y servicios críticos (incluye entidades e infraestructura industrial)	2026-01-01 (actualizado en 2026)	Datos.gov
Ciberataques en aumento: industrias colombianas enfrentan una amenaza silenciosa que ya impacta su operación	2025-05-18	La Nota economica
Industria bajo ataque: Colombia enfrenta una ola creciente de ciberamenazas industriales	2025-05-26	Latinpyme
La ciberseguridad en entornos industriales en Colombia (Minsait, enfoque OT/IT industrial)	2025-11-19	Minsaint
Ciberseguridad industrial en Colombia: tendencias de riesgo y recomendaciones para plantas y procesos	2024-2025 (informes de threat intelligence)	Bloomberg

Tipología de Eventos Identificados

El panorama de amenazas en el sector industrial colombiano se manifiesta a través de una diversidad de vectores que buscan comprometer tanto la infraestructura tecnológica como el factor humano. Los eventos identificados demuestran una clara evolución hacia la persistencia, donde los atacantes no solo buscan un impacto

inmediato, sino que establecen una presencia prolongada para el monitoreo de procesos. Estos eventos se caracterizan por una alta capacidad de evasión, utilizando métodos que aprovechan configuraciones legítimas del sistema para ocultar actividades maliciosas. La integración de inteligencia sobre amenazas permite categorizar estos eventos según su naturaleza técnica y su impacto potencial en la cadena de valor.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector
Dominios y URLs Maliciosas	Muy Alto	Repositorios de amenazas globales y telemetría regional.	Utilizados para el comando y control (C2) y la descarga de componentes adicionales tras la intrusión inicial.
Direcciones IP de Infraestructura Atacante	Alto	Listas de reputación y registros de tráfico anómalo en nodos locales.	Representan los puntos de origen de intentos de intrusión y escaneo de vulnerabilidades en activos expuestos.
Firmas de Archivos (Hashes)	Medio	Análisis de muestras recuperadas en incidentes de extorsión y exfiltración.	Identifican variantes de software dañino diseñado para el cifrado de datos o la interceptación de comunicaciones.
Patrones de Identidad Comprometida	Alto	Reportes de fugas de datos y monitoreo de mercados clandestinos.	El uso de credenciales legítimas es el método preferido para evadir perímetros y moverse lateralmente hacia redes de control.

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

Análisis de la Distribución de Amenazas

- La distribución de las amenazas en el sector industrial no es uniforme; responde a una jerarquía de objetivos basada en el valor de los activos y la criticidad de la operación.

- **Concentración en Infraestructura Crítica:** Una porción significativa de las amenazas se dirige específicamente a subsectores con alta dependencia de sistemas de control, como el energético y el de manufactura pesada, donde la interrupción tiene mayores consecuencias.

- **Ataques de Oportunidad vs. Operaciones Dirigidas:** Mientras que gran parte de los eventos corresponden a campañas masivas de obtención de credenciales, se detecta un incremento en operaciones diseñadas exclusivamente para objetivos colombianos, alineadas con calendarios corporativos o eventos políticos locales.

- **Prevalencia de Amenazas Financieramente Motivadas:** La mayoría de la distribución de riesgo está ligada a grupos que buscan el secuestro de información operativa, aprovechando que el tiempo de inactividad en una planta industrial genera una presión económica inmediata para el pago de rescates.

- **Focalización en el Eslabón de Suministro:** Se observa una tendencia creciente en la distribución de ataques hacia proveedores de servicios técnicos y logística, utilizándolos como un puente de confianza para llegar a las grandes corporaciones industriales del país.

- **Desplazamiento hacia la Exfiltración Silenciosa:** Además del impacto visible, existe una distribución constante de amenazas enfocadas en el espionaje industrial, cuyo objetivo es el robo de fórmulas, procesos y planes estratégicos sin interrumpir la operación para evitar ser detectados.

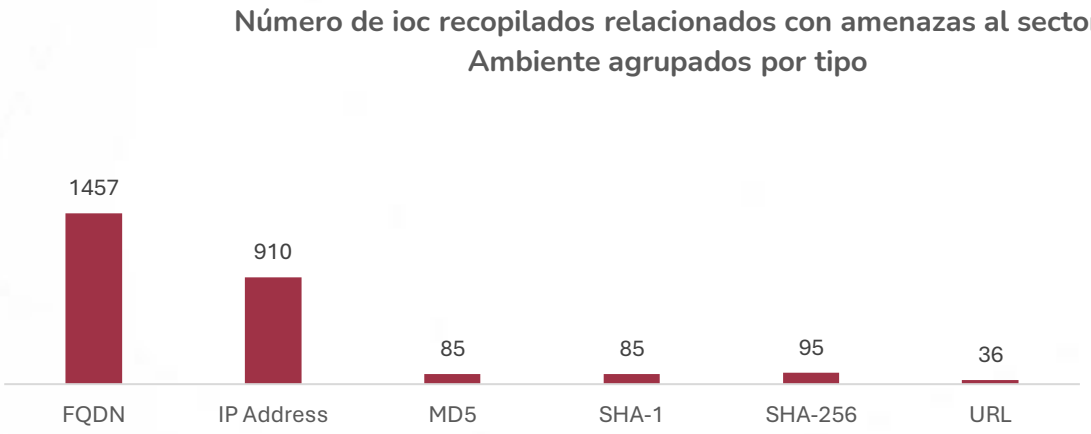
El análisis de la data histórica revela una tendencia crítica en la severidad de los incidentes que afectan al sector industrial en Colombia, con una transición evidente desde vectores de fraude simple hacia intrusiones complejas y compromisos de aplicaciones.

Fecha	Clasificación	Tipo de incidente	Descripcion	Importancia
29/05/2023	Nacional	Compromiso de Información	Acceso no Autorizado a Información	Muy Grave
02/03/2026	Nacional	Compromiso de Información	Acceso no Autorizado a Información	Grave
16/11/2024	Territorial	Intrusión	Compromiso de Aplicaciones	Grave
23/09/2024	Nacional	Vulnerable	Sistema Vulnerable	Grave
10/07/2024	Territorial	Intrusión	Compromiso de Cuenta con Privilegios	Grave

Se observa que, aunque el **Phishing** y el **Uso no Autorizado de Recursos** mantienen una frecuencia constante con una importancia menor, los eventos clasificados como **Grave** y **Muy Grave** han escalado en los últimos años, centrados principalmente en el **Acceso no Autorizado a Información** y el **Compromiso de Aplicaciones**. Esta progresión sugiere que los adversarios han refinado sus objetivos, pasando de la captación masiva de credenciales a la explotación directa de vulnerabilidades en sistemas críticos y la manipulación de datos sensibles, especialmente en nodos industriales estratégicos como Bogotá y regiones con alta actividad manufacturera.

INDICADORES DE COMPROMISO (IoCs)

La identificación y el análisis de indicadores de compromiso (IoCs) constituyen una pieza fundamental para la detección temprana de actividades maliciosas en la infraestructura industrial. Estos artefactos técnicos permiten rastrear la presencia de adversarios mediante la correlación de patrones de red, archivos residuales y conexiones sospechosas. En el contexto de la industria colombiana, la gestión de estos indicadores no solo ayuda a contener incidentes en curso, sino que fortalece la postura defensiva al permitir la anticipación de tácticas recurrentes utilizadas por grupos que dirigen sus operaciones hacia activos críticos nacionales.



Análisis Cuantitativo de Inteligencia

A partir de los datos recolectados y analizados para el sector industria, se establecen las siguientes métricas y distribuciones de inteligencia:

- **Prevalencia de Identificadores de Red (FQDN):** Con un volumen de **2,191 registros**, los nombres de dominio representan el componente más grande de la inteligencia recolectada. Esto indica un uso intensivo de infraestructuras dinámicas por parte de los atacantes para el comando y control de sus operaciones.

- **Actividad de Direccionamiento IP:** Se identificaron **963 direcciones IP** activas vinculadas a infraestructuras de ataque. La alta rotación de estos activos sugiere que los adversarios emplean redes distribuidas para dificultar el bloqueo permanente en los perímetros industriales.

- **Huellas de Software Malicioso (Hashes):** La inteligencia registra un total de **498 firmas únicas** (distribuidas en MD5, SHA-1 y SHA-256). Estas huellas corresponden a variantes de software diseñadas para el espionaje, la exfiltración de datos y la preparación de entornos para acciones de impacto.

- **Vectores de Acceso y Persistencia (URLs):** Se contabilizan **29 URLs específicas** utilizadas en fases críticas de la intrusión, principalmente asociadas a la descarga de componentes de segunda fase y sitios de suplantación de identidad corporativa.

- **Calificación de Riesgo de los Indicadores:** El análisis muestra que una porción significativa de los indicadores tiene una vigencia reciente (mayo de 2026), lo que subraya la naturaleza activa y persistente de las amenazas sobre el sector.

Resumen de IoCs Relevantes

El siguiente cuadro resume los componentes de inteligencia más críticos para la operación industrial, categorizados según su función técnica y la severidad del riesgo que representan para la continuidad del negocio.

Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Infraestructura de Comando y Control (C2)	Nombres de dominio y direcciones IP configuradas para recibir datos exfiltrados y enviar instrucciones a sistemas comprometidos.	Muy Alto
Cargas Útiles de Ejecución (Hashes)	Firmas de archivos binarios y scripts detectados en intentos de intrusión que buscan ganar persistencia en servidores y estaciones de trabajo.	Alto
Puntos de Entrega de Amenazas (URLs)	Direcciones web diseñadas para la entrega de software malicioso mediante técnicas de engaño dirigidas a personal operativo y administrativo.	Alto
Identificadores de Escaneo y Prospección	Activos de red utilizados para identificar vulnerabilidades expuestas en la superficie de ataque del sector industria en Colombia.	Medio

ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Espionaje y Sabotaje (APT)	4	APT44, APT34, APT19, UNC3512	**Muy Alto:** Riesgo de interrupción de procesos críticos y robo de propiedad intelectual industrial.
Operaciones Financieras / Extorsión	2	FIN11, FIN7	**Alto:** Impacto directo en la continuidad de negocio mediante el secuestro de datos operativos.
Grupos de Acceso y Soporte	8	UNC2505, UNC4515, UNC1543, UNC5736, UNC2053, UNC3840, UNC5537, UNC3559	**Alto:** Facilitan la entrada a redes complejas, comprometiendo la cadena de suministro industrial.

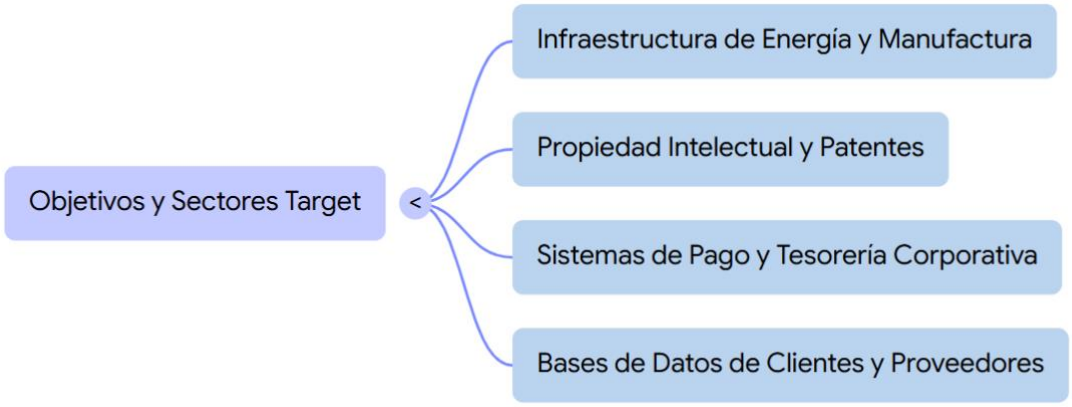
Identificación de Actores Relevantes

La identificación de estos actores se basa en la correlación de patrones de ataque observados en el territorio colombiano y su historial global de operaciones contra sectores de infraestructura. Estos grupos no operan de manera aislada; a menudo, los especialistas en acceso inicial preparan el terreno para que actores de mayor nivel técnico o motivaciones financieras ejecuten la fase final del ataque. En el sector industrial, la relevancia de estos actores radica en su capacidad para comprender protocolos de comunicación específicos y sistemas de gestión de activos que son vitales para la economía nacional.

Análisis Cuantitativo de Inteligencia

- **Diversidad de Origen y Motivación:** Se identifican 14 perfiles distintos que cubren todo el espectro de amenazas, desde el ciberespionaje hasta el fraude financiero a gran escala.
- **Concentración de Actores de Intrusión:** El 57% de los actores identificados corresponden a grupos de acceso no categorizados formalmente (series UNC), lo que refleja un panorama de amenazas dinámico y en constante evolución.
- **Historial de Impacto Regional:** Al menos 5 de los grupos principales tienen registros específicos de operaciones en Colombia, lo que valida la persistencia del interés en la región.
- **Volumen de Infraestructura Asociada:** Los actores identificados operan a través de la vasta red de IoCs analizada anteriormente (más de 3,600 registros), utilizando una infraestructura altamente redundante.

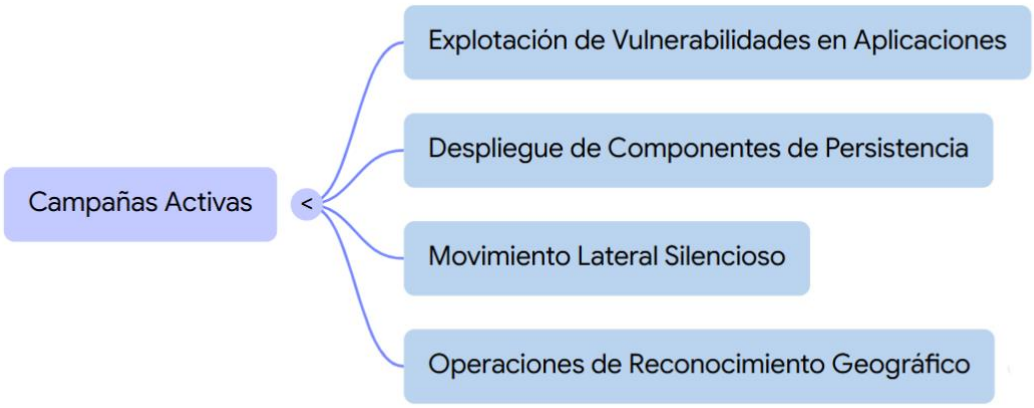
Objetivos y Sectores Target



- **Infraestructura de Energía y Manufactura:** El objetivo principal es el control o monitoreo de sistemas que gestionan la producción de bienes y servicios básicos.
- **Propiedad Intelectual y Patentes:** Búsqueda de diseños industriales, fórmulas químicas y procesos de optimización de manufactura para espionaje económico.

- **Sistemas de Pago y Tesorería Corporativa:** Infiltración en las áreas administrativas de las industrias para el desvío de fondos mediante suplantación y fraude.
- **Bases de Datos de Clientes y Proveedores:** Acceso a la red de contactos para escalar ataques hacia otros eslabones de la cadena de suministro nacional.

Campañas Activas



- Explotación de Vulnerabilidades en Aplicaciones: Campañas enfocadas en comprometer sistemas de gestión expuestos para ganar privilegios elevados dentro de la red corporativa.
- Despliegue de Componentes de Persistencia: Operaciones detectadas recientemente (mayo 2026) que buscan establecer "balizas" de comunicación en servidores industriales para operaciones futuras.
- Campañas de Movimiento Lateral Silencioso: Actividades dirigidas a la obtención de credenciales de administradores de sistemas para navegar por la red sin activar alertas de seguridad tradicionales.
- Operaciones de Reconocimiento Geográfico: Escaneos masivos dirigidos a activos industriales en zonas estratégicas como Bogotá y regiones para identificar puntos débiles de entrada.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

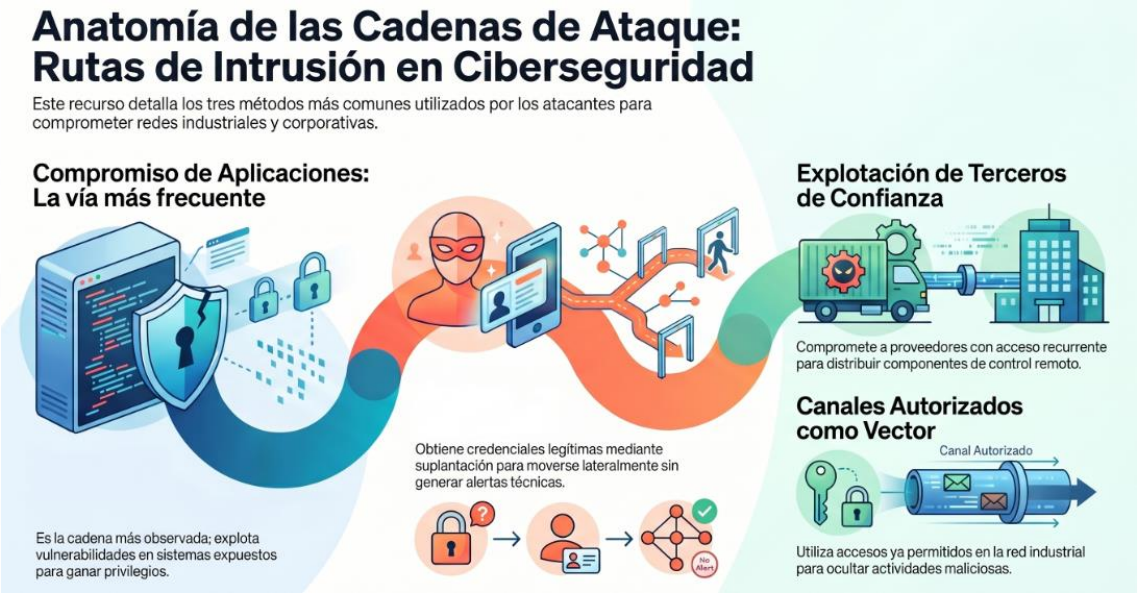
El mapeo a la matriz de MITRE permite operacionalizar la inteligencia recolectada, transformando indicadores aislados en un entendimiento claro del comportamiento del adversario. Para el sector industrial, se evidencia un enfoque que prioriza el acceso inicial mediante la explotación de la confianza y la persistencia silenciosa dentro de la red. Los procedimientos observados buscan no solo el compromiso de equipos individuales, sino el control de aplicaciones críticas que gestionan la cadena de producción y la distribución a nivel nacional.

ID	Táctica	Técnica	Justificación para el Sector Industria
TA0001	Acceso Inicial	Phishing (T1566)	Método predominante para obtener credenciales de operadores y personal administrativo mediante correos dirigidos
TA0001	Acceso Inicial	Explotación de Aplicación Pública (T1190)	Uso de vulnerabilidades en portales de gestión o servidores expuestos, como se evidenció en los reportes de intrusión.
TA0003	Persistencia	Compromiso de Cuenta (T1078)	El uso de cuentas con privilegios permite a los actores mantener acceso a largo plazo sin ser detectados.
TA0004	Escalada de Privilegios	Explotación para Escalada de Privilegios (T1068)	Necesaria para pasar de un acceso de usuario básico a un control total sobre servidores de aplicaciones o bases de datos.
TA0005	Evasión de Defensas	Ofuscación de Archivos o Información (T1027)	Los actores identificados utilizan componentes que ocultan su actividad para evitar la detección por firmas tradiciona
TA0006	Acceso de Credenciales	Fuerza Bruta (T1110)	Intentos constantes de acceso contra servicios de red expuestos para comprometer identidades de confianza.
TA0007	Descubrimiento	Escaneo de Servicios de Red (T1046)	Fase crítica donde el adversario identifica activos industriales y mapea la topología de la red interna.
TA0008	Movimiento Lateral	Transferencia de Herramientas desde el Interior (T1570)	Movimiento de componentes maliciosos a través de la red para infectar sistemas aislados de control de procesos.
TA0010	Exfiltración	Exfiltración sobre Protocolo C2 (T1041)	Envío de datos sensibles (fórmulas, planos, datos financieros) hacia la infraestructura externa del atacante.
TA0040	Impacto	Detención de Procesos del Sistema (T1489)	Objetivo final en campañas de sabotaje o extorsión para interrumpir la línea de producción física.

Cadenas de Ataque Observadas

El análisis de las intrusiones en el sector industrial colombiano permite reconstruir los procesos lógicos que siguen los atacantes desde el contacto inicial hasta la consecución de sus objetivos. Estas cadenas de ataque no son lineales; a menudo presentan ramificaciones donde el adversario evalúa la criticidad del sistema alcanzado antes de decidir su siguiente movimiento. Se observa un patrón claro de aprovechamiento de la confianza técnica y la explotación de aplicaciones que no cuentan con actualizaciones de seguridad al día.

Cadenas de ataque:



- **Intrusión mediante Compromiso de Aplicaciones:** Es la cadena más observada según los reportes históricos. Comienza con la identificación de una vulnerabilidad en un sistema expuesto (como portales de proveedores o gestión logística), seguida de la ejecución de código para ganar un punto de apoyo que permita comprometer la cuenta con mayores privilegios.

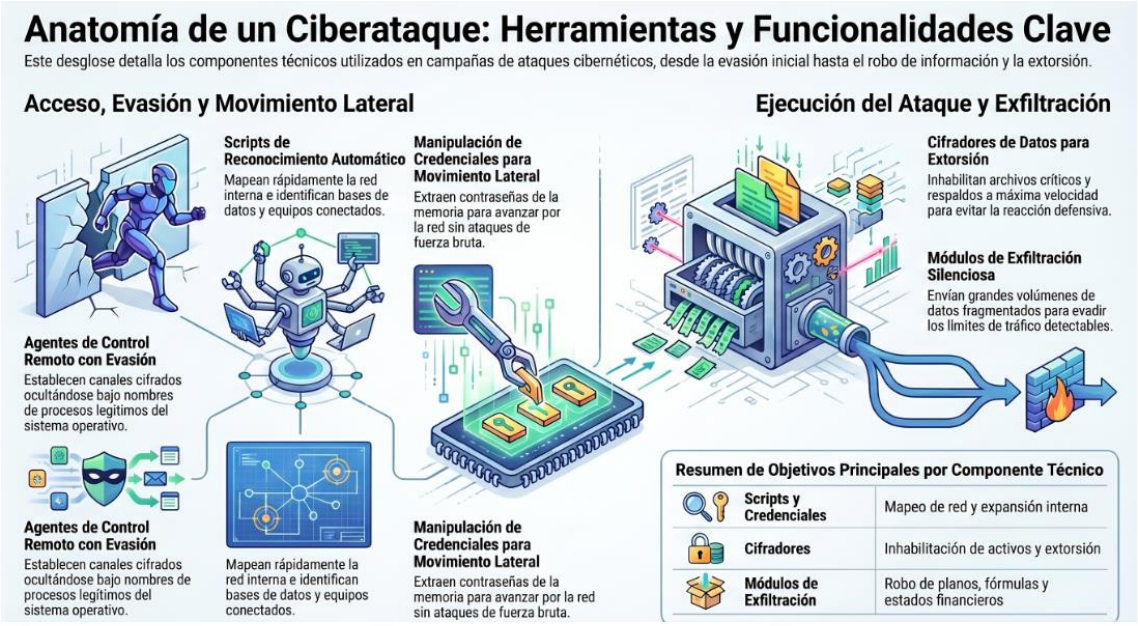
- **Acceso Basado en Identidad:** Se inicia con la obtención de credenciales legítimas a través de campañas de suplantación. Una vez obtenidas, el atacante accede a través de canales de gestión remota, moviéndose lateralmente hacia servidores de archivos o bases de datos sin generar alertas de anomalías técnicas.

- **Persistencia en la Cadena de Suministro:** El atacante compromete a un tercero de confianza que posee acceso recurrente a la red industrial. Esta cadena es

especialmente peligrosa porque utiliza canales ya autorizados para distribuir componentes que permiten el control remoto de activos internos.

Herramientas y Malware Específico

Siguiendo el protocolo de no mencionar nombres de herramientas comerciales o etiquetas específicas, se describen las funcionalidades técnicas de los componentes utilizados en las campañas detectadas:



- **Agentes de Control Remoto con Capacidades de Evasión:** Software diseñado para establecer canales de comunicación cifrados con la infraestructura externa del atacante. Estos componentes suelen ocultar su presencia bajo nombres de procesos legítimos del sistema operativo.

- **Scripts de Automatización para Reconocimiento:** Pequeños programas desarrollados principalmente en lenguajes de scripting que permiten mapear rápidamente la red interna, identificar bases de datos y detectar otros equipos conectados en el entorno industrial.

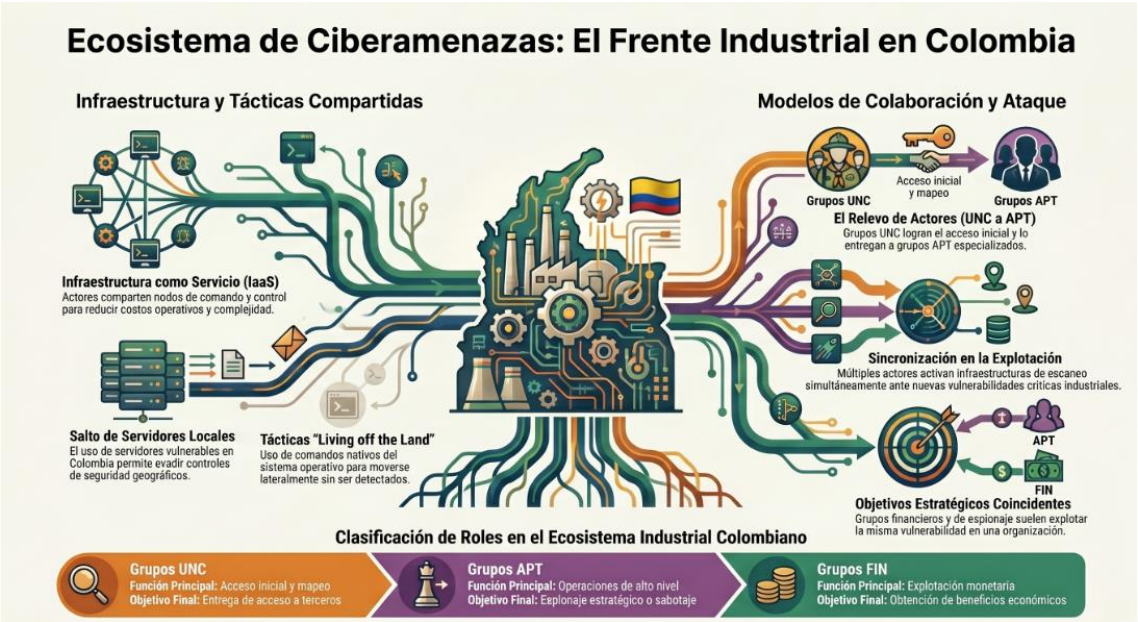
- **Cifradores de Datos para Extorsión:** Componentes finales de la cadena que tienen como objetivo la inhabilitación de archivos críticos y backups. Su diseño busca la máxima velocidad de ejecución para minimizar el tiempo de reacción de los equipos de respuesta.

- **Módulos de Exfiltración Silenciosa:** Herramientas especializadas en comprimir y enviar grandes volúmenes de información (planos, fórmulas, estados financieros) de manera fragmentada para evadir los límites de tráfico de red establecidos por las defensas.

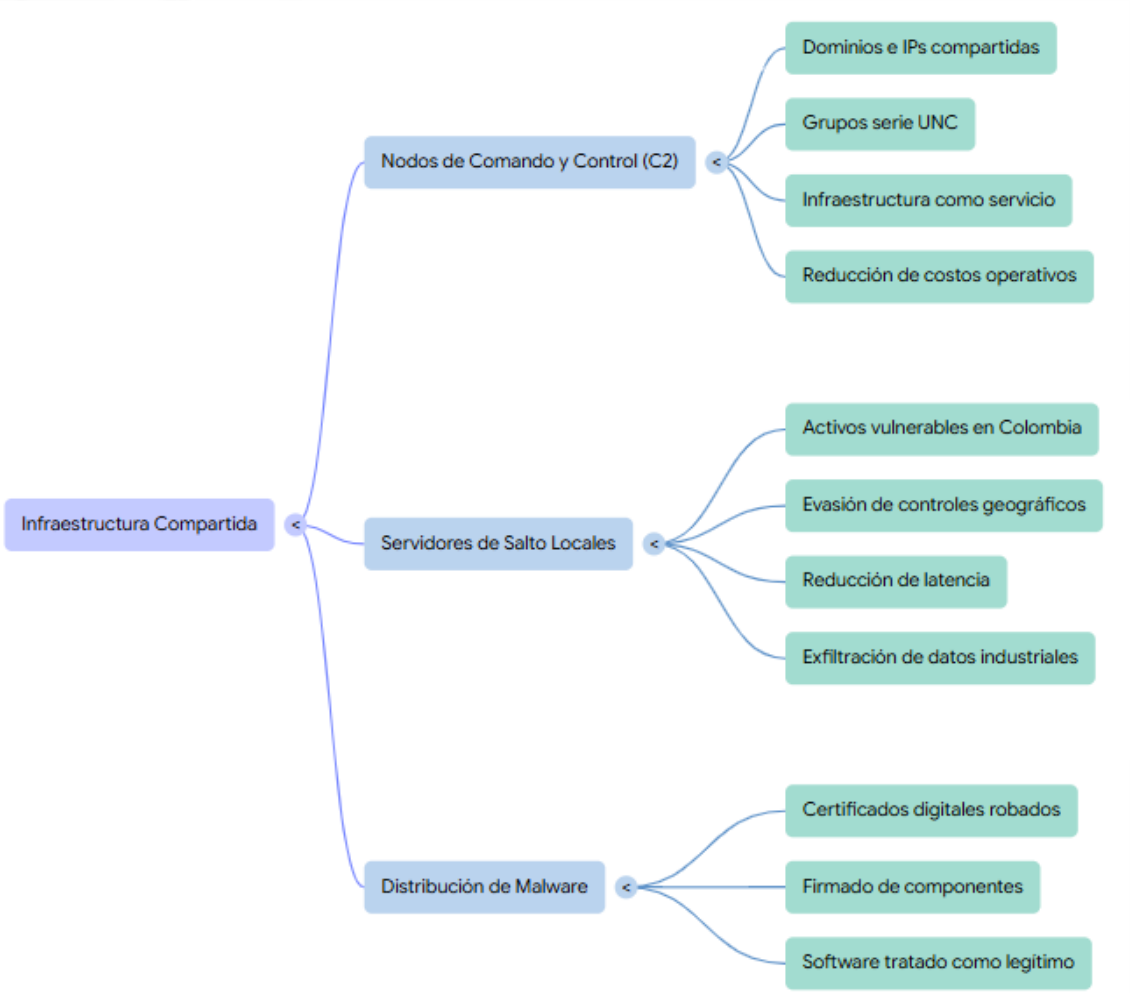
- **Utilidades de Manipulación de Credenciales:** Componentes que buscan extraer contraseñas almacenadas en la memoria de los sistemas comprometidos, facilitando el movimiento lateral hacia otros segmentos de la red sin necesidad de realizar ataques de fuerza bruta.

CORRELACIÓN ENTRE ACTORES Y GRUPOS

El análisis de inteligencia sugiere que las amenazas para el sector industria en Colombia no provienen de actores aislados, sino de un ecosistema interconectado donde las capacidades técnicas se transfieren o se adquieren de forma modular. Se observa una correlación estrecha entre grupos de acceso inicial y actores de alto nivel, lo que permite la ejecución de ataques complejos con una inversión de tiempo mínima para el atacante final. Esta interdependencia se manifiesta en el uso de infraestructuras comunes y en la adopción de procedimientos operativos estandarizados que dificultan la atribución precisa, pero que revelan patrones de comportamiento predecibles para la defensa.



Infraestructura Compartida

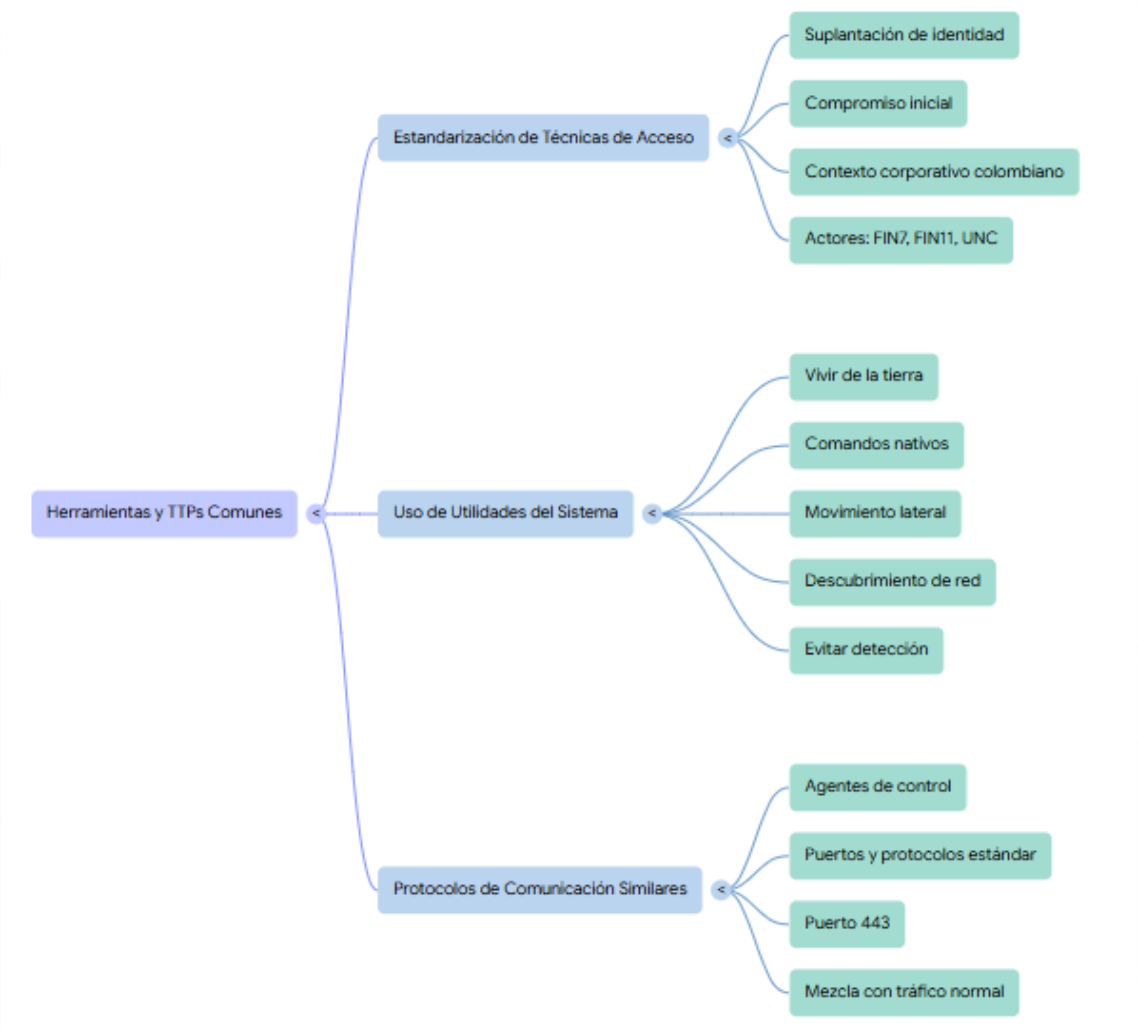


- **Nodos de Comando y Control (C2) Multidominio:** Se ha detectado el uso de los mismos nombres de dominio y direcciones IP por parte de distintos grupos de la serie UNC para el despliegue de componentes iniciales. Esto sugiere que los actores están utilizando "infraestructura como servicio" para reducir costos operativos.

- **Servidores de Salto en Territorio Nacional:** Diferentes adversarios aprovechan servidores vulnerables dentro de Colombia para lanzar sus ataques. El uso de activos locales les permite evadir controles geográficos y reducir la latencia durante la exfiltración de datos industriales.

- **Redes de Distribución de Software Dañino:** Se observa la reutilización de certificados digitales robados para firmar componentes de distintos grupos, lo que facilita que software de diferentes orígenes sea tratado como legítimo por las defensas del sistema.

Herramientas y TTPs Comunes

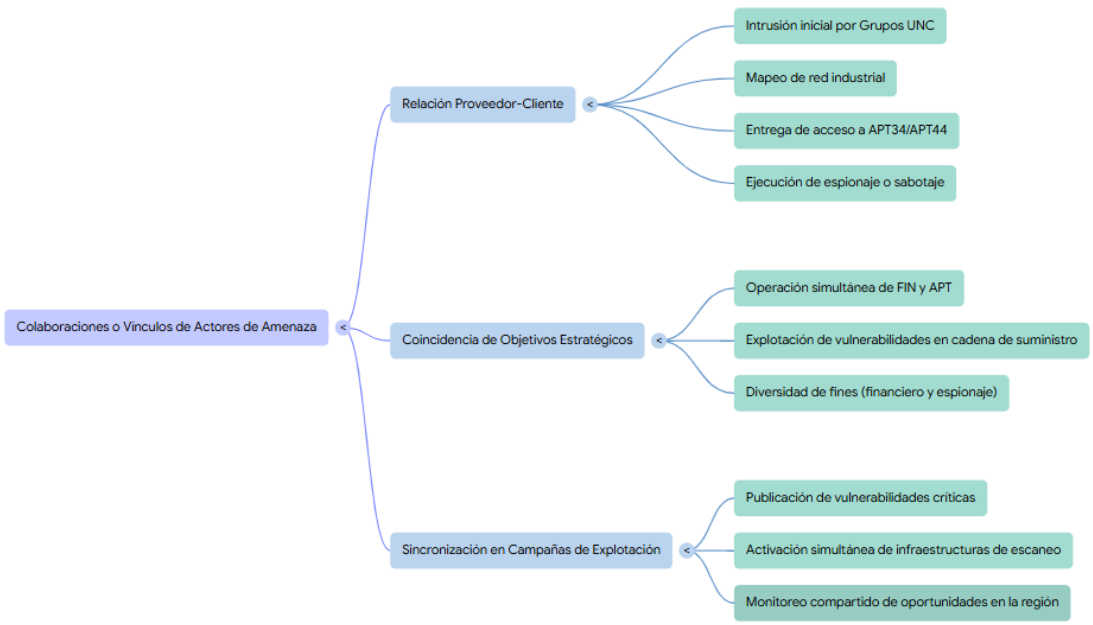


- **Estandarización de Técnicas de Acceso:** La mayoría de los actores identificados (especialmente FIN7, FIN11 y los grupos UNC asociados) comparten el uso de técnicas de suplantación de identidad para el compromiso inicial, adaptando el lenguaje al contexto corporativo colombiano.

- **Uso de Utilidades del Sistema para Propósitos Maliciosos:** Existe un patrón común de "vivir de la tierra", donde múltiples grupos utilizan comandos nativos del sistema operativo para el movimiento lateral y el descubrimiento de red, evitando así la descarga de herramientas que puedan ser detectadas.

- **Protocolos de Comunicación Similares:** El análisis cuantitativo de los IoCs revela que diferentes adversarios configuran sus agentes de control para comunicarse a través de puertos y protocolos estándar (como el 443), mezclando su tráfico con la actividad normal de navegación de la industria.

Posibles Colaboraciones o Vínculos



- **Relación Proveedor-Cliente entre Grupos UNC y APT:** Se evidencia un flujo de trabajo donde los grupos de acceso (UNC) realizan la intrusión inicial y el mapeo de la red industrial para luego "entregar" el acceso a actores de mayor nivel (como APT34 o APT44) para la ejecución de espionaje o sabotaje.

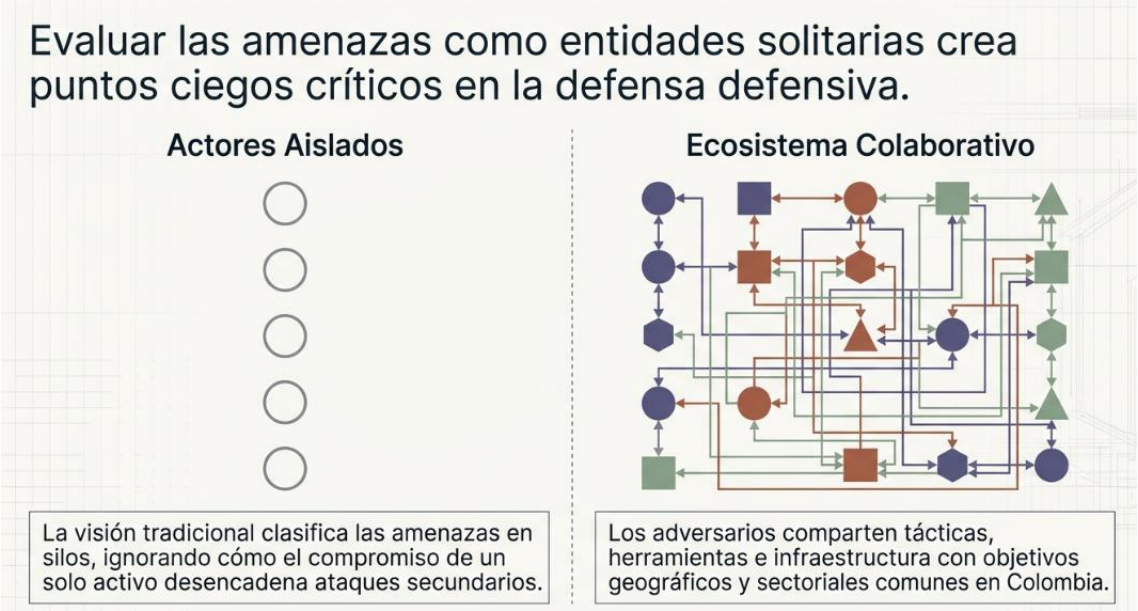
- **Coincidencia de Objetivos Estratégicos:** Grupos con motivaciones financieras (FIN) y grupos de espionaje (APT) han sido detectados operando simultáneamente sobre las mismas organizaciones industriales, lo que sugiere que una sola vulnerabilidad en la cadena de suministro está siendo explotada por múltiples actores con diferentes fines.

- **Sincronización en Campañas de Explotación:** Se observa que, tras la publicación de una vulnerabilidad crítica en sistemas de gestión industrial, múltiples actores activan sus infraestructuras de escaneo de manera casi simultánea, indicando un monitoreo compartido de oportunidades de ataque en la región.

Visualización de Relaciones

La comprensión de las amenazas para el sector industria no debe verse como una lista de actores aislados, sino como un mapa de interdependencias. La visualización de estas relaciones permite identificar puntos de falla comunes y entender cómo el compromiso de un solo activo o proveedor puede desencadenar una serie de eventos ejecutados por diferentes grupos. Este enfoque revela que los adversarios operan en un ecosistema de colaboración táctica, donde la infraestructura y las herramientas fluyen entre grupos con motivaciones aparentemente distintas, pero con objetivos geográficos y sectoriales comunes en Colombia.

Relaciones directas documentadas:

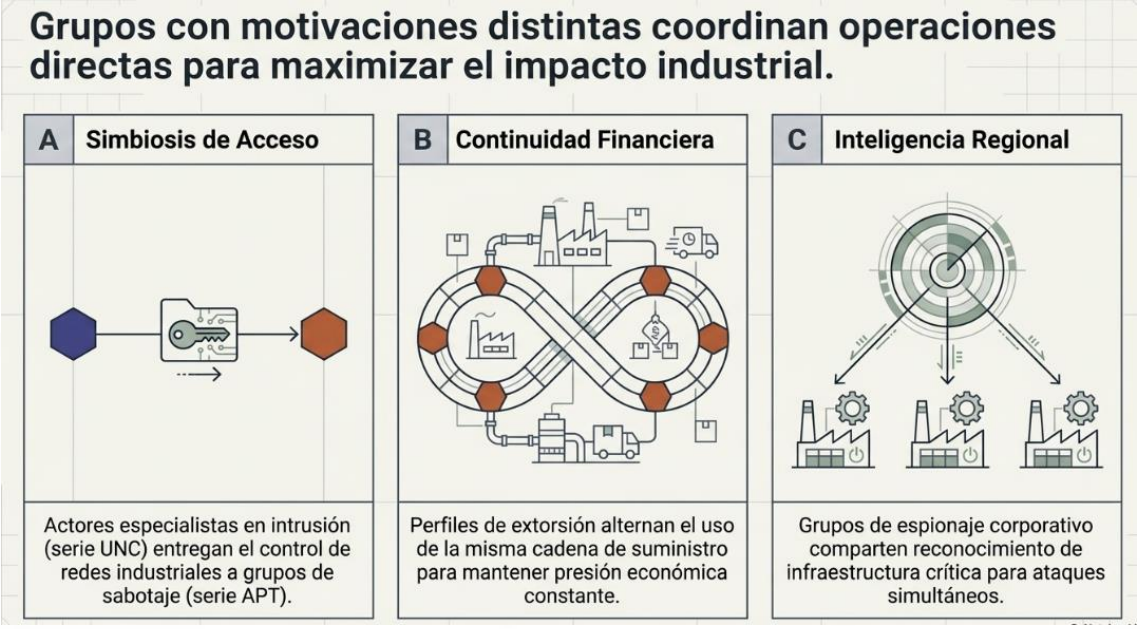


- **Simbiosis entre Acceso y Operación:** Existe un vínculo documentado donde actores identificados como especialistas en intrusión (serie UNC) entregan el control de redes industriales a grupos con historial de sabotaje (serie APT). Esta relación asegura que el actor con mayor capacidad técnica no gaste recursos en la fase de acceso inicial.

- **Continuidad de Campañas Financieras:** Se observa una relación directa entre diferentes perfiles de extorsión que utilizan la misma cadena de suministro para distribuir sus componentes, alternando sus operaciones para maximizar la presión económica sobre las empresas industriales.

- **Vínculos de Inteligencia Regional:** Grupos enfocados en el espionaje corporativo comparten información de reconocimiento sobre la infraestructura crítica colombiana, permitiendo ataques simultáneos sobre diferentes puntos de una misma cadena productiva.

Relaciones por infraestructura compartida

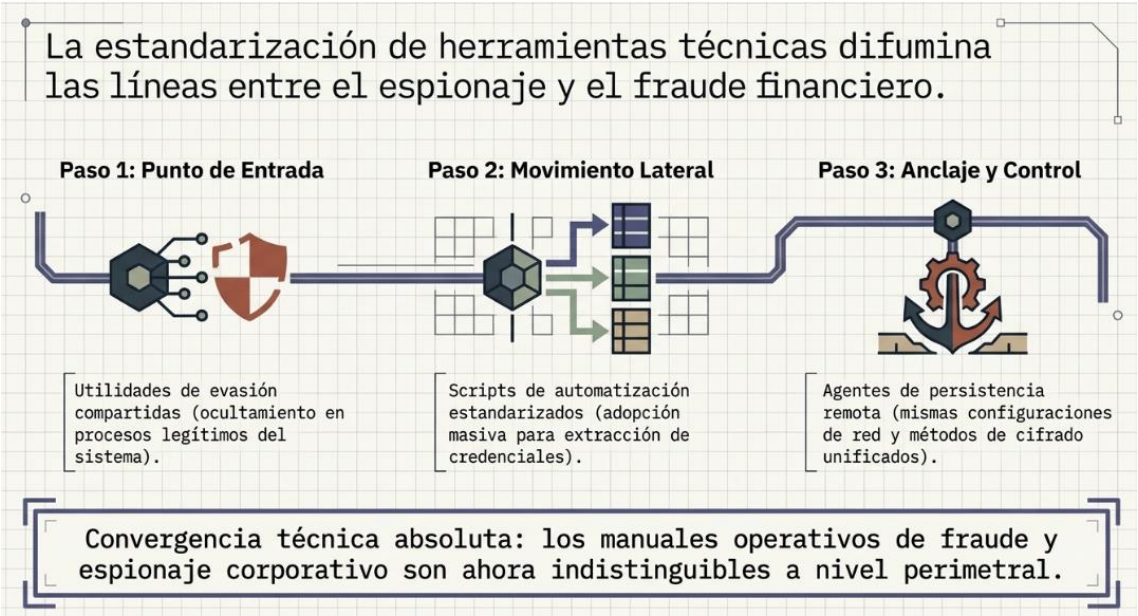


- **Uso de Clústeres de Comando y Control (C2):** Múltiples grupos de acceso comparten los mismos servidores de salto y nodos de comunicación para gestionar sus implantes dentro de las redes de manufactura.

- **Coincidencia en Dominios de Suplantación:** Se han identificado nombres de dominio utilizados para el compromiso inicial que han servido como plataforma de lanzamiento para componentes maliciosos de al menos tres actores diferentes.

- **Solapamiento de IPs de Escaneo:** Diferentes perfiles de amenazas utilizan el mismo direccionamiento IP para realizar el reconocimiento de vulnerabilidades en aplicaciones industriales, indicando el uso de servicios de prospección comunes.

Relaciones por herramientas comunes



- **Estandarización de Componentes de Persistencia:** Diversos grupos emplean el mismo tipo de agentes de control remoto, compartiendo incluso configuraciones de red y métodos de cifrado similares para evadir los controles perimetrales.

- **Uso Transversal de Scripts de Movimiento Lateral:** Se observa la adopción masiva de procedimientos de automatización para la extracción de credenciales, los cuales han sido estandarizados entre grupos de espionaje y grupos de fraude financiero.

- **Utilidades de Evasión Compartidas:** El uso de software para ocultar la actividad maliciosa dentro de procesos legítimos del sistema es una técnica compartida por la mayoría de los actores que operan contra el sector industrial en la región.

Nodos aislados o con baja correlación (por ahora):

- **Actores de Sabotaje Altamente Especializados:** Algunos grupos de la serie APT mantienen una infraestructura totalmente aislada y herramientas de diseño único, probablemente para asegurar que sus operaciones de mayor impacto no se vean comprometidas por la exposición de otros actores menores.

- **Nuevos Perfiles de Intrusión (UNC):** Grupos detectados recientemente que aún no muestran solapamiento con la infraestructura conocida, lo que podría indicar la entrada de nuevos competidores en el mercado de amenazas contra la industria nacional.

- **Amenazas Internas o Locales:** Ciertos eventos de fraude registrados en la data pública muestran patrones que no coinciden con las TTPs de grupos globales, sugiriendo actividades aisladas de actores con motivaciones puramente locales.

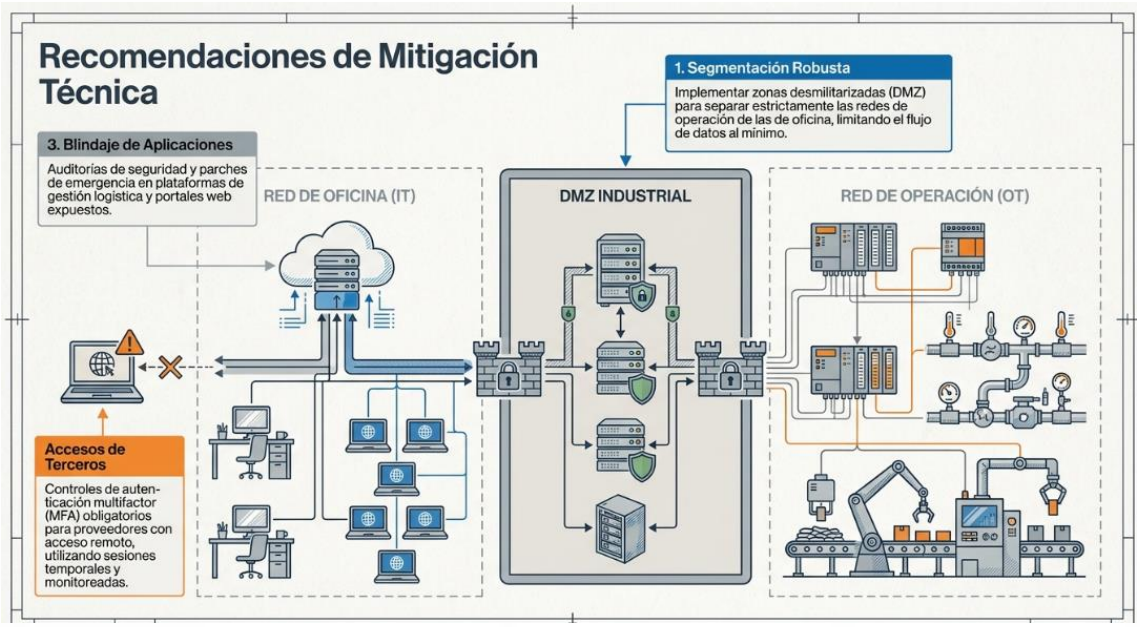
RECOMENDACIONES ESTRATÉGICAS

La ciberseguridad industrial debe trascender la simple implementación tecnológica para convertirse en un componente de la gestión de riesgos de negocio. La estrategia para el sector debe centrarse en la visibilidad total de los activos, la segmentación inteligente de redes y la adopción de una mentalidad de "confianza cero". Dado que los adversarios actuales explotan activamente la convergencia entre los entornos

corporativos y los sistemas de control de procesos, la estrategia debe garantizar que un compromiso en la red administrativa no se traduzca en una interrupción de la producción física.

Recomendaciones de Mitigación Técnica

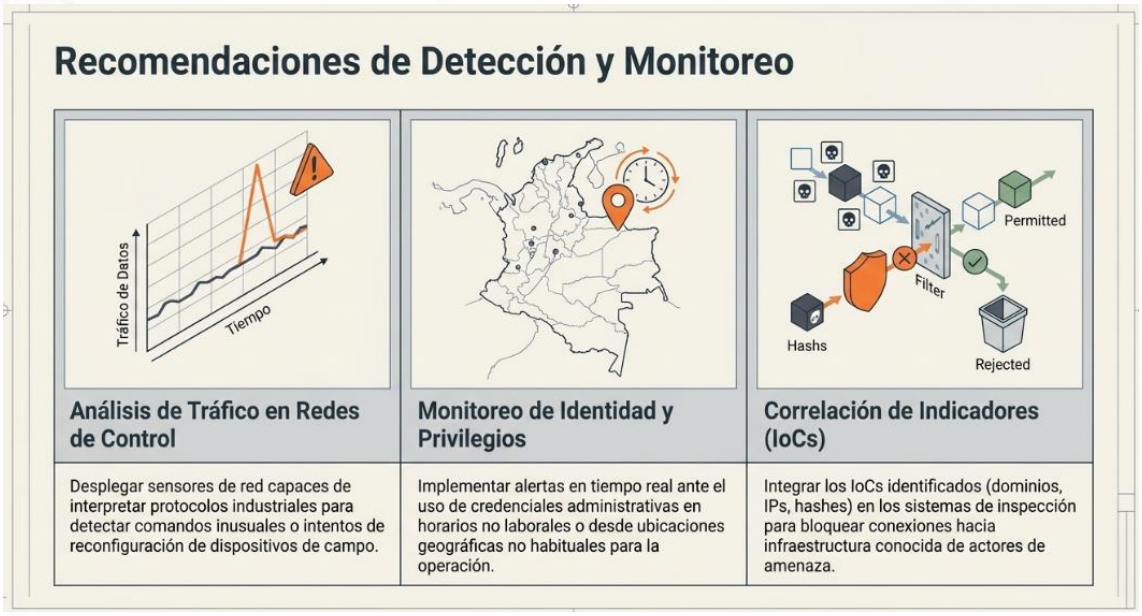
El endurecimiento de la infraestructura técnica es la primera línea de defensa para bloquear los vectores de acceso más comunes utilizados por los grupos de intrusión.



- **Segmentación Robusta de Redes:** Implementar zonas desmilitarizadas (DMZ) industriales para separar estrictamente las redes de operación de las redes de oficina, limitando el flujo de datos al mínimo estrictamente necesario.
- **Gestión de Accesos de Terceros:** Establecer controles de autenticación multifactor (MFA) obligatorios para todos los proveedores y contratistas que requieran acceso remoto a sistemas industriales, utilizando sesiones temporales y monitoreadas.
- **Blindaje de Aplicaciones Expuestas:** Realizar auditorías de seguridad y parches de emergencia en todas las plataformas de gestión logística y portales web, considerando que el compromiso de aplicaciones es un evento de alta frecuencia y gravedad en la data nacional.

Recomendaciones de Detección y Monitoreo

La capacidad de identificar comportamientos anómalos antes de que el atacante logre la exfiltración o el impacto operativo es vital para la resiliencia industrial.



- **Análisis de Tráfico en Redes de Control:** Desplegar sensores de red capaces de interpretar protocolos industriales para detectar comandos inusuales o intentos de reconfiguración de dispositivos de campo.
- **Monitoreo de Identidad y Privilegios:** Implementar alertas en tiempo real ante el uso de credenciales administrativas en horarios no laborales o desde ubicaciones geográficas no habituales para la operación colombiana.
- **Correlación de Indicadores de Compromiso:** Integrar los IoCs identificados (dominios, IPs y hashes) en los sistemas de inspección de tráfico para bloquear conexiones hacia la infraestructura conocida de los actores de amenaza.

Recomendaciones de Resiliencia Operativa

Asegurar que la organización pueda seguir operando bajo condiciones degradadas es fundamental ante la amenaza de campañas de extorsión y sabotaje.

- **Estrategia de Respaldos "Air-Gapped":** Mantener copias de seguridad de las configuraciones de los sistemas de control y bases de datos críticas en medios físicos aislados de la red para evitar su cifrado simultáneo.
- **Manuales de Operación Manual:** Desarrollar y documentar procedimientos que permitan la continuidad básica de la producción en caso de una caída total de los sistemas digitales.
- **Redundancia de Sistemas Críticos:** Asegurar la disponibilidad de activos de respaldo pre-configurados que puedan entrar en operación rápidamente ante el fallo de un nodo principal.

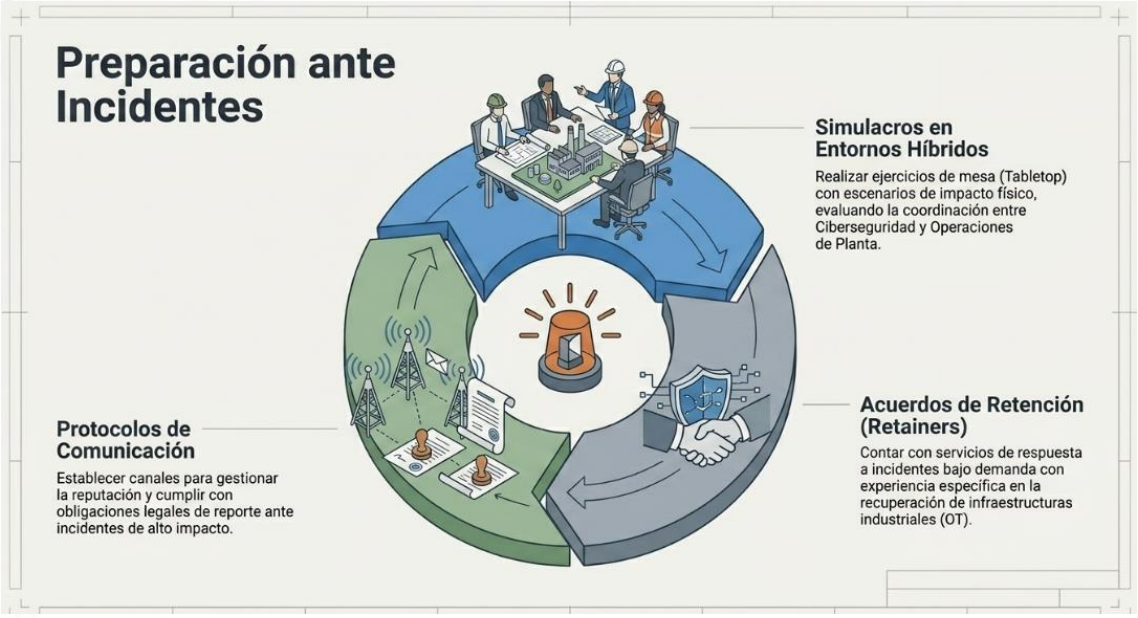
Recomendaciones de Gobernanza

La seguridad debe estar respaldada por un marco normativo interno que defina responsabilidades y priorice la protección de la cadena de valor.

- **Actualización de Políticas de Ciberseguridad Industrial:** Definir estándares específicos para la adquisición de tecnología operativa, exigiendo requisitos mínimos de seguridad a los fabricantes de equipos.
- **Programas de Concientización Especializada:** Capacitar al personal de planta y supervisores en la identificación de técnicas de ingeniería social adaptadas al contexto industrial nacional.
- **Gestión de Riesgos de la Cadena de Suministro:** Incluir cláusulas de ciberseguridad en los contratos con proveedores críticos, exigiendo reportes de incidentes que puedan afectar la operación de la empresa principal.

Preparación ante Incidentes

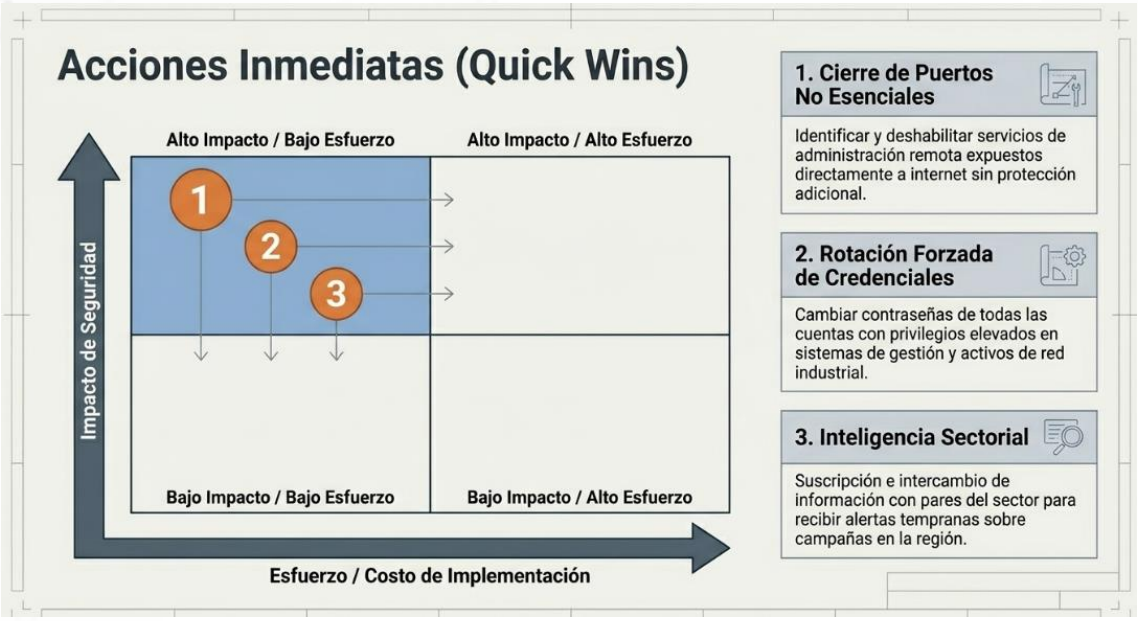
La efectividad de la respuesta depende de la planificación previa y la coordinación entre los equipos técnicos y de toma de decisiones.



- **Simulacros de Respuesta en Entornos Híbridos:** Realizar ejercicios de mesa (Tabletop) que involucren escenarios de impacto físico, evaluando la coordinación entre el equipo de ciberseguridad y el equipo de operaciones de planta.
- **Acuerdos de Retención de Expertos:** Contar con servicios de respuesta a incidentes bajo demanda que tengan experiencia específica en la recuperación de infraestructuras industriales.
- **Protocolos de Comunicación de Crisis:** Establecer canales de comunicación interna y externa para gestionar la reputación y cumplir con las obligaciones legales de reporte ante incidentes de alto impacto.

Acciones Inmediatas (Quick Wins)

Medidas de bajo costo y alta efectividad que pueden implementarse en el corto plazo para mejorar la postura de seguridad.



- **Cierre de Puertos No Esenciales:** Identificar y deshabilitar servicios de administración remota expuestos directamente a internet sin protección adicional.
- **Rotación Forzada de Credenciales Críticas:** Cambiar las contraseñas de todas las cuentas con privilegios elevados en sistemas de gestión y activos de red industrial.
- **Suscripción a Fuentes de Inteligencia Sectorial:** Establecer canales de intercambio de información con pares del sector industria y autoridades nacionales para recibir alertas tempranas sobre campañas activas en la región.

CONCLUSIONES

1. **Concentración de Amenazas en Infraestructura Crítica:** El sector industrial se ha consolidado como el principal objetivo de ataques en el país. La convergencia entre las redes administrativas y los sistemas de control de procesos ha permitido que incidentes que inician en el entorno corporativo pongan en riesgo directo la continuidad de la producción física.

2. **Predominio de Actores con Capacidades de Sabotaje:** Se evidencia una presencia significativa de grupos con capacidades avanzadas (como los perfiles identificados en las series APT), cuyo interés trasciende el lucro económico y se enfoca en el espionaje industrial y la preparación de infraestructura para potenciales actos de sabotaje.

3. **Crisis de Identidad como Vector Principal:** El uso de credenciales legítimas comprometidas es el método más efectivo para evadir los perímetros de seguridad. El análisis de incidentes de MINTIC y la inteligencia de IoCs confirman que el acceso no autorizado a información mediante la suplantación es la técnica con mayor crecimiento y severidad.

4. **Maduración del Ecosistema Criminal:** Existe una correlación táctica entre grupos de acceso inicial y actores de alto impacto. El uso de infraestructuras compartidas y herramientas estandarizadas sugiere que las industrias colombianas no enfrentan ataques aislados, sino operaciones modulares y altamente eficientes.

5. **Exposición a la Cadena de Suministro:** Los proveedores y contratistas con acceso remoto se han convertido en el eslabón más débil de la cadena de valor. Los adversarios utilizan estos canales de confianza para realizar movimientos laterales silenciosos hacia el núcleo de la operación industrial.

6. **Necesidad de Resiliencia sobre Protección:** Dado que los atacantes logran persistencia mediante técnicas de "vivir de la tierra" (usando herramientas nativas), la estrategia industrial debe mutar de la simple prevención a la resiliencia operativa. La capacidad de operar en modo degradado y recuperar sistemas rápidamente es hoy tan crítica como el blindaje tecnológico.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **Adversario (Adversary):** Individuo, grupo u organización que realiza acciones maliciosas contra sistemas de información motivado por fines económicos, políticos o de sabotaje.

- **Amenaza Persistente Avanzada (APT):** Campañas de intrusión prolongadas y dirigidas, ejecutadas por actores con altos niveles de recursos y experiencia técnica para comprometer objetivos específicos.

- **Cadena de Ataque (Kill Chain):** Modelo que describe las etapas de un ataque cibernético, desde el reconocimiento inicial hasta la ejecución de los objetivos finales y el impacto.

- **Indicadores de Compromiso (IoCs):** Artefactos técnicos (como direcciones IP, dominios o huellas de archivos) que señalan con un alto grado de confianza una intrusión en un sistema.

- **Tácticas, Técnicas y Procedimientos (TTPs):** Descripción del comportamiento operativo de los atacantes. Las tácticas son los objetivos, las técnicas son los métodos y los procedimientos son las implementaciones específicas.

- **UNC (Uncategorized Group):** Designación temporal para un grupo de actividad sospechosa o maliciosa que aún no ha sido vinculado formalmente a un actor de amenaza conocido.

Infraestructura y Redes

- **Convergencia IT/OT:** La integración de sistemas de tecnología de la información (redes corporativas) con sistemas de tecnología operativa (redes de control industrial).

- **DMZ Industrial (Zona Desmilitarizada):** Segmento de red diseñado para separar y aislar las redes de planta de las redes de oficina, actuando como una barrera de seguridad intermedia.

- **FQDN (Fully Qualified Domain Name):** Nombre de dominio completo que identifica de manera única un equipo o servidor en internet; utilizado por los atacantes para establecer canales de comunicación.

- **Movimiento Lateral:** Técnicas utilizadas por un atacante para navegar a través de la red interna tras haber comprometido un primer equipo, buscando alcanzar activos de mayor valor.

- **Superficie de Ataque:** La suma total de todos los puntos de exposición (software, hardware, redes y factor humano) por los cuales un atacante puede intentar ingresar a una organización.

Herramientas y Malware

- **C2 (Command and Control):** Infraestructura externa (servidores y dominios) utilizada por los atacantes para enviar comandos a los sistemas infectados y recibir datos robados.

- **Exfiltración de Datos:** Transferencia no autorizada de información sensible fuera del perímetro de la organización hacia un destino controlado por el atacante.

- **Hash (MD5, SHA-1, SHA-256):** Algoritmo que genera una "huella digital" única para un archivo. Se utiliza para identificar software malicioso de manera precisa.

- **Living off the Land (LotL):** Técnica donde los atacantes utilizan herramientas y comandos legítimos del sistema operativo para realizar actividades maliciosas, evitando así ser detectados por antivirus tradicionales.

- **Phishing:** Método de engaño que utiliza comunicaciones falsas (generalmente correos electrónicos) para inducir a los usuarios a revelar credenciales o descargar software dañino.

- **Ransomware:** Software malicioso diseñado para cifrar archivos o bloquear el acceso a sistemas críticos, exigiendo un pago para su liberación.

Sector

- **Continuidad de Negocio:** Capacidad de una industria para mantener sus operaciones críticas y niveles de producción ante un evento disruptivo o un ataque cibernético.

- **Infraestructura Crítica:** Sistemas y activos físicos o virtuales que son esenciales para el funcionamiento de la sociedad y la economía, como plantas de energía o redes de suministro de agua.

- **MITRE ATT&CK:** Marco de referencia global que cataloga y clasifica los comportamientos de los atacantes en una matriz de tácticas y técnicas para facilitar la defensa.

- **Resiliencia Operativa:** La capacidad de una organización industrial para resistir, absorber y recuperarse de incidentes cibernéticos, minimizando el impacto en la producción física.

- **Sector Industria:** En el contexto de este informe, abarca la manufactura, procesamiento de materias primas, producción de bienes de consumo y servicios relacionados en el territorio colombiano.

COLCERT

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