TIC

Informe de apreciación

Sector Agua

COLCERT

Informe de apreciación Sector Agua

COLCERT IN-20260709-041

TLP: CLEAR

Contenido

COLCERT
La información contenida en este documento, bajo clasificación TLP:CLEAR - -Pública puede ser utilizada y compartida libremente con fines informativos, técnicos y de prevención, siempre que se cite como fuente al **Equipo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT).**
Uso permitido con atribución. © ColCERT, 2026.

Informe de apreciación Sector Agua

COLCERT IN-20260709-041

TLP: CLEAR

RESUMEN EJECUTIVO

En el sector de agua y saneamiento básico en Colombia, la transformación digital y la integración de sistemas de control operativo (OT) han ampliado significativamente la exposición a ciberamenazas. Actores de persistencia avanzada (APT), grupos de cibercrimen organizado y operadores de ransomware dirigen sus ataques hacia estas infraestructuras críticas, buscando comprometer la continuidad del suministro, la integridad de los procesos de potabilización y la prestación de servicios esenciales para la población.

Este informe utiliza inteligencia de amenazas de vanguardia para realizar un seguimiento riguroso al comportamiento de los actores que afectan el sector, a partir de la correlación de información técnica y táctica recopilada. Se priorizan fuentes de alta fidelidad (abiertas, comerciales e institucionales) que aportan visibilidad estratégica sobre amenazas relevantes para las infraestructuras críticas nacionales, permitiendo una toma de decisiones informada frente al riesgo digital.

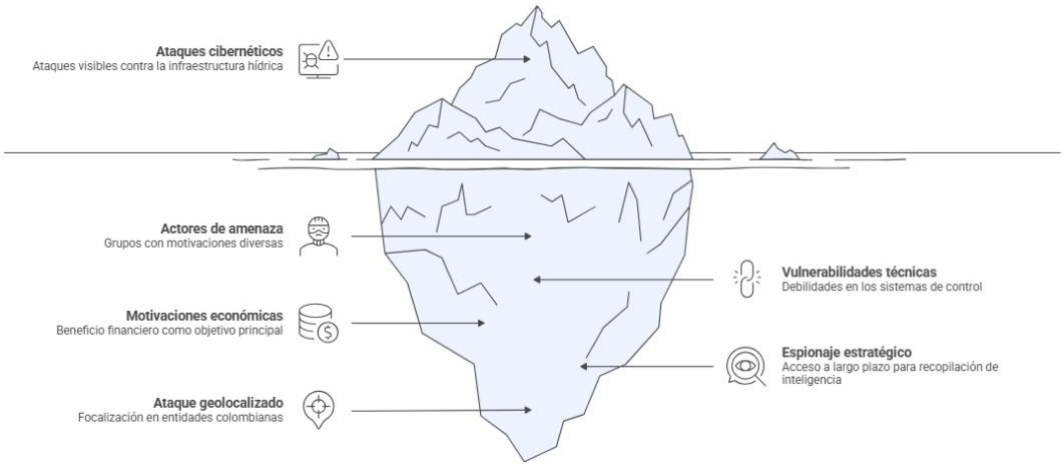
Lineamientos

- ✓ **Seguimiento a actores** que afectan el sector hídrico y de saneamiento en Colombia.
- ✓ **Uso de inteligencia de amenazas** para la identificación proactiva de vectores de ataque.
- ✓ **Priorización de fuentes** de ciberinteligencia aplicables al contexto y geografía del país.
- ✓ **Enfoque en infraestructuras críticas** nacionales y sistemas de control industrial (ICS).
- ✓ **Reducción de tiempos de detección** y respuesta ante incidentes de alto impacto.
- ✓ **Fortalecimiento de la resiliencia** cibernética de las entidades prestadoras de servicios públicos.

Informe de apreciación Sector Agua

COLCERT IN-20260709-041

TLP: CLEAR



INTRODUCCIÓN

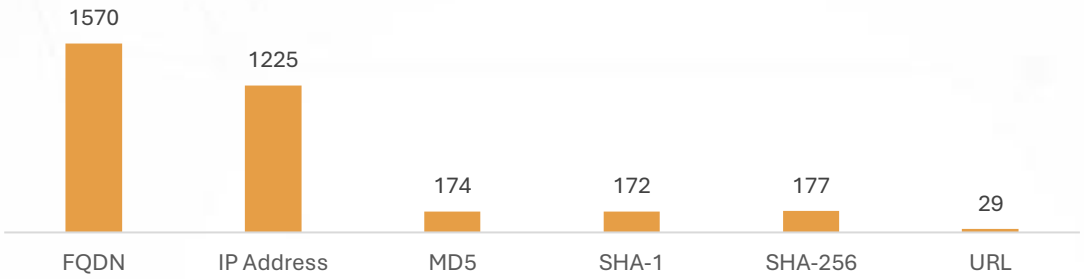
El panorama de amenazas para el sector Agua en Colombia durante el último periodo refleja un interés sostenido por parte de diversos actores de amenazas con motivaciones que oscilan entre el espionaje estratégico y el beneficio económico. La infraestructura crítica del país se encuentra en un punto de convergencia donde la digitalización de los sistemas de control operativo aumenta la superficie de exposición ante grupos con capacidades avanzadas de intrusión y persistencia.

Puntos Clave:

- ✓ Identificación de múltiples grupos con historial de ataques a infraestructuras críticas operando en la región.
- ✓ Persistencia de tácticas de compromiso inicial mediante técnicas de ingeniería social y explotación de activos expuestos.
- ✓ Presencia de actores especializados en el despliegue de cargas útiles financieras y robo de información sensible.
- ✓ Riesgo latente de interrupción operativa mediante el acceso a redes de gestión y control.

Hallazgos Clave

Malware, actores y C2 identificadas: insumos para la ciberseguridad del sector Agua en Colombia

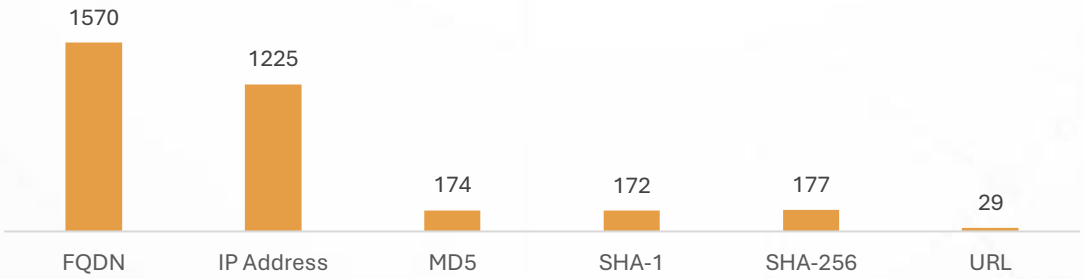


- ✓ **Actores de Amenaza Persistente:** Se ha detectado la actividad de grupos de alta sofisticación técnica que históricamente han dirigido sus esfuerzos hacia sectores de servicios públicos a nivel global, lo que sugiere un riesgo elevado para la integridad de los sistemas hídricos nacionales.

- ✓ **Diversidad de Motivaciones:** La telemetría analizada revela una combinación de amenazas; mientras algunos grupos buscan el acceso a largo plazo para recolección de inteligencia, otros se enfocan en la distribución de software malicioso diseñado para la extorsión financiera

- ✓ **Vector de Ataque Geolocalizado:** Existe una clara focalización en entidades colombianas, lo que indica que los adversarios están ajustando sus campañas para evadir controles locales y aprovechar las vulnerabilidades específicas de la infraestructura tecnológica del país.

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



Recomendaciones Prioritarias

- ✓ Segregación de Redes: Implementar y reforzar la separación física o lógica entre las redes de gestión administrativa y los entornos de control industrial (OT) para evitar el movimiento lateral de posibles intrusos.
- ✓ Monitoreo de Acceso Identitario: Robustecer las políticas de autenticación de múltiples factores y realizar auditorías exhaustivas sobre las cuentas con privilegios elevados que gestionan activos críticos.
- ✓ Gestión de Vulnerabilidades en Activos Expuestos: Priorizar el cierre de brechas de seguridad en servicios orientados a internet, los cuales son frecuentemente utilizados como punto de entrada inicial por los grupos identificados.

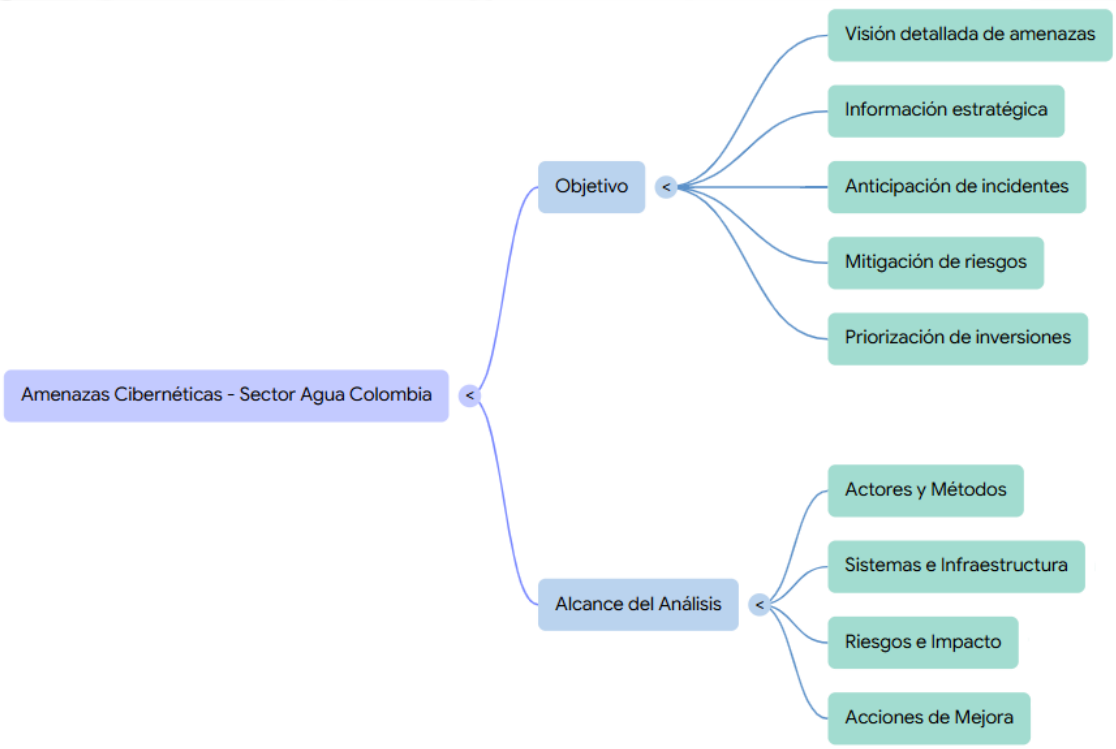
Conclusión Estratégica

El sector Agua en Colombia enfrenta un desafío de seguridad multidimensional. La presencia de adversarios con capacidades comprobadas para afectar la continuidad de los servicios públicos requiere que las organizaciones del sector dejen de ver la seguridad informática como una función de soporte y la integren como un pilar de la resiliencia operativa. La protección de los recursos hídricos es una cuestión de seguridad nacional, y la postura defensiva debe evolucionar hacia la detección temprana y la respuesta proactiva ante amenazas dirigidas.

OBJETIVO Y ALCANCE

Objetivo

El presente informe tiene como propósito fundamental proporcionar una visión clara y detallada sobre las amenazas cibernéticas que impactan directamente al sector Agua en Colombia. Se busca dotar a los responsables de la toma de decisiones de información estratégica que permita anticipar incidentes, mitigar riesgos y priorizar las inversiones en seguridad para salvaguardar la prestación del servicio vital.



Alcance

Este análisis abarca la actividad de los principales actores de amenaza identificados con intereses en el territorio colombiano durante el trimestre actual. El enfoque comprende el estudio de sus métodos de operación, objetivos probables y el impacto potencial sobre los activos de información y sistemas de control que componen la cadena de valor del agua y el saneamiento básico en el país.

Este informe abarca:

- ✓ Actividad de actores de amenaza con presencia en el territorio colombiano.
- ✓ Infraestructura tecnológica y sistemas de gestión del sector hídrico.
- ✓ Vectores de compromiso inicial y métodos de intrusión detectados.
- ✓ Impacto potencial en la continuidad de servicios públicos esenciales.
- ✓ Tendencias de ciberespionaje y motivaciones económicas contra infraestructuras críticas.
- ✓ Medidas de mitigación técnica y estratégica para el fortalecimiento operativo.

CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR

Definición y Entendimiento del Sector

El sector de Agua y Saneamiento Básico en Colombia es un pilar fundamental de la infraestructura crítica nacional, encargado de garantizar el acceso, tratamiento y distribución del recurso hídrico, así como la disposición de aguas residuales. Este sector se caracteriza por una alta dependencia tecnológica, donde convergen redes administrativas y sistemas de automatización industrial que permiten el control remoto de plantas de tratamiento, estaciones de bombeo y embalses. Dada su naturaleza vital para la salud pública y la estabilidad económica, cualquier alteración en su funcionamiento no solo genera un impacto financiero, sino que constituye un riesgo directo para la seguridad y el bienestar de la población en las diversas regiones del territorio.

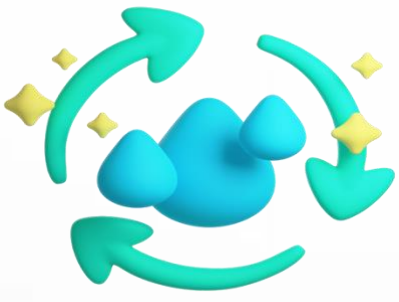
Superficie de Ataque

La superficie de ataque del sector ha experimentado una expansión significativa debido a la integración de tecnologías digitales en procesos que anteriormente eran manuales. Esta interconectividad, si bien optimiza la operación, crea múltiples puntos de entrada que pueden ser explotados por los actores de amenaza identificados. Los principales vectores de exposición incluyen:

- ✓ **Sistemas de Control Industrial (ICS/SCADA):** Dispositivos y protocolos que gestionan físicamente la infraestructura de agua; su exposición a redes externas aumenta el riesgo de sabotaje o manipulación operativa.
- ✓ **Interfaces de Gestión Remota:** El uso de accesos remotos para mantenimiento y supervisión técnica que, de no estar debidamente protegidos, sirven como puerta de entrada para el compromiso de credenciales.
- ✓ **Infraestructura en la Nube y Servicios Web:** Portales de atención al ciudadano, sistemas de facturación y almacenamiento de datos sensibles que son objetivos primordiales para el robo de información.
- ✓ **Cadena de Suministro Tecnológica:** Dependencia de proveedores externos de software y hardware, cuya vulnerabilidad puede ser utilizada para infiltrar las redes principales de las organizaciones hídricas.
- ✓ **Dispositivos de Borde y Redes Administrativas:** Equipos de oficina y servidores de correo que suelen ser el primer eslabón en ataques de ingeniería social o distribución de software malicioso.

PANORAMA ACTUAL DE AMENAZAS

El escenario de ciberseguridad para el sector de agua y saneamiento en Colombia se encuentra en un estado de alerta elevada, caracterizado por un incremento sostenido en la sofisticación y frecuencia de las incursiones digitales. Según datos recientes, el país ha experimentado un crecimiento del **30%** en ataques dirigidos a entidades de servicios públicos, donde la convergencia entre los sistemas de gestión comercial y la infraestructura operativa ha sido explotada por grupos con capacidades avanzadas.



TITULO	FECHA	FUENTE / ENLACE
Protegiendo las infraestructuras de agua y saneamiento de amenazas cibernéticas (informe para América Latina y Caribe, con enfoque en Colombia)	2023-07-10	Colombia Inteligente
Ciberseguridad en el sector hídrico: casos y riesgos para infraestructuras de agua y saneamiento	Sin fecha específica (documento 202x)	Agua.unam
El sector del agua también debe protegerse frente a los ciberataques (visión general para infraestructuras de agua y saneamiento)	Varía según fuente secundaria	yahoo
Gestión de Incidentes en Colombia (incluye incidentes cibernéticos de servicios públicos como agua)	2026-01-01 (actualizado en 2026)	Datos.gov
Ataques cibernéticos han crecido 30% y EPM y Sanitas son dos de miles (caso de empresa de servicios públicos, incluyendo agua)	2022-12-13	La Republica

Tipología de Eventos Identificados

El análisis de los datos recolectados revela una actividad diversa que abarca desde la recolección pasiva de inteligencia hasta intentos directos de intrusión. Los eventos se caracterizan por el uso de infraestructura de comando y control altamente volátil y el despliegue de artefactos maliciosos diseñados para evadir soluciones de seguridad convencionales. La mayoría de los incidentes detectados inician con fases de reconocimiento sobre activos expuestos, seguidas por intentos de acceso mediante credenciales comprometidas o explotación de vulnerabilidades en servicios de red.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector
Direcciones IP (C2)	Alto	Reportes de inteligencia global y telemetría de red.	**Crítica**: Representan intentos de comunicación con servidores externos para exfiltración o control.
Hashes de Malware	Medio	Repositorios de amenazas y análisis de muestras locales.	**Alta**: Identifican herramientas de persistencia y software de cifrado (extorsión).
Dominios Maliciosos	Medio	Registros de DNS y campañas de ingeniería social.	**Alta**: Utilizados en ataques de suplantación dirigidos a empleados del sector.
Patrones de Tráfico (Protocolos)	Bajo	Monitoreo de redes industriales (OT).	**Muy Alta**: Indican posibles intentos de manipulación en sistemas de control de plantas y bombeo.

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

Análisis de la Distribución de Amenazas

A partir de la tipología presentada, se extraen las siguientes conclusiones clave sobre el comportamiento de los eventos en el sector:

- Predominancia de Infraestructura C2: El volumen "Muy Alto" de indicadores de Comando y Control (C2) sugiere que existen intentos persistentes de establecer persistencia dentro de las redes del sector para futuras fases de ataque.
- Convergencia de Riesgos TI/TO: Los hallazgos de malware con criticidad alta indican una amenaza directa hacia la disponibilidad de los sistemas de control industrial, donde un compromiso puede derivar en fallas físicas de suministro.
- Sofisticación en la Evasión: La presencia de dominios DGA y acortadores resalta la necesidad de contar con sistemas de detección dinámica, ya que los atacantes están utilizando infraestructuras efímeras para evadir listas negras estáticas tradicionales.
- Enfoque en el Robo de Identidad: El alto volumen de phishing y suplantación confirma que el eslabón humano (operadores y personal administrativo) sigue siendo el vector preferido para obtener acceso inicial a las redes corporativas.

El registro histórico de eventos para las entidades vinculadas a la gestión ambiental y del recurso hídrico en Colombia revela una tendencia crítica hacia la **intrusión mediante el compromiso de aplicaciones** y la persistencia de **sistemas vulnerables**, especialmente en nodos centrales como Bogotá y regiones clave como Santander y Antioquia. Se observa que, aunque los eventos de fraude (como el phishing) son frecuentes, los incidentes clasificados como "Graves" están directamente relacionados con la pérdida de control sobre activos tecnológicos y el acceso no autorizado a información sensible, lo que pone de manifiesto una brecha en la gestión de parches y en la robustez de las aplicaciones orientadas a la red.

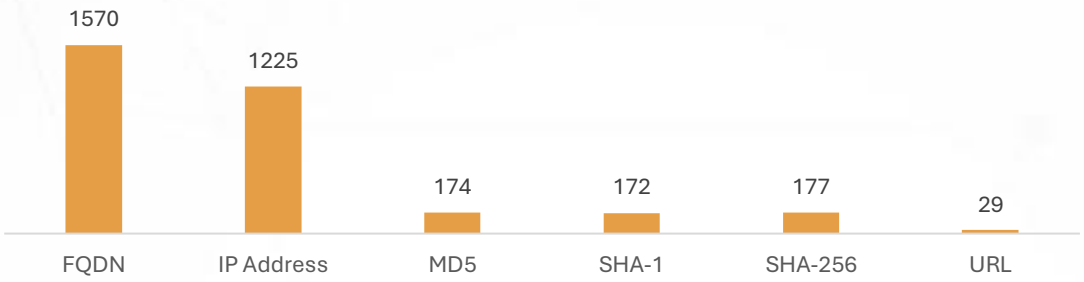
Fecha	Clasificación	Tipo de Incidente	Descripción	Importancia
6/03/2026	Territorial	Vulnerable	Sistema Vulnerable	Grave
27/11/2025	Nacional	Intrusión	Compromiso de Aplicaciones	Grave
31/07/2025	Territorial	Vulnerable	Sistema Vulnerable	Grave
14/07/2025	Territorial	Intrusión	Compromiso de Aplicaciones	Grave
11/07/2025	Territorial	Intrusión	Compromiso de Aplicaciones	Grave

Este ranking resalta que el **Compromiso de Aplicaciones** y la presencia de **Sistemas Vulnerables** no solo son los incidentes más comunes, sino que también representan la mayor amenaza para la continuidad operativa. La recurrencia de estos eventos sugiere que los actores de amenaza están priorizando la explotación de fallos técnicos sobre la interacción humana directa en esta etapa del monitoreo.

INDICADORES DE COMPROMISO (IoCs)

Los Indicadores de Compromiso representan la evidencia técnica de una intrusión o intento de compromiso en la infraestructura. En el contexto del sector Agua, estos indicadores permiten identificar la presencia de los actores de amenaza previamente analizados (como grupos de persistencia avanzada y actores financieros). El monitoreo y bloqueo proactivo de estos IoCs es fundamental para interrumpir la cadena de ataque antes de que se logre un impacto en los sistemas de control operativo o en la integridad de los datos de los usuarios.

Número de IOC recopilados con amenazas al sector Agua agrupados por tipo



Análisis Cuantitativo de Inteligencia

- ✓ Prevalencia de Infraestructura de Comando y Control (C2): Se observa un alto volumen de direcciones IP vinculadas a servidores de control externo, lo que sugiere intentos constantes de establecer persistencia tras una intrusión inicial.
- ✓ Sofisticación de Artefactos Maliciosos: La distribución de hashes únicos indica el uso de herramientas personalizadas o modificadas para evadir firmas de seguridad estándar, elevando la dificultad de detección.
- ✓ Temporalidad de los Ataques: Los datos muestran picos de actividad que coinciden con periodos de actualización de sistemas o ventanas de mantenimiento, lo que indica un monitoreo activo por parte de los adversarios.
- ✓ Diversidad de Protocolos: Se ha identificado el uso de protocolos no estándar para la comunicación saliente, una táctica común para eludir sistemas de prevención de intrusiones (IPS) tradicionales.

Resumen de IoCs Relevantes

A continuación, se describen los componentes de inteligencia clave identificados en las campañas dirigidas a infraestructuras críticas en la región y su valoración de riesgo asociada.

Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Direcciones IP de Redes Externas	Nodos identificados como origen de escaneos de vulnerabilidades y puntos de terminación para túneles de datos.	Crítico
Hashes de Archivos (SHA-256)	Firmas digitales de archivos ejecutables y scripts maliciosos utilizados para la recolección de credenciales.	Alto
Dominios de Suplantación (Look-alike)	Nombres de dominio que imitan a entidades gubernamentales y de servicios públicos para campañas de engaño.	Alto
Patrones de Tráfico Anomalos	Intentos de conexión hacia puertos de gestión (RDP, SSH) desde geografías no habituales para la operación.	Muy Alto
Cadenas de User-Agents Específicas	Identificadores de navegadores y herramientas automatizadas utilizadas por grupos de persistencia avanzada.	Medio

ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Persistencia Avanzada (APT)	4	APT44, APT34, APT19, UNC3559	**Crítico:** Capacidad de sabotaje a infraestructuras de control y espionaje prolongado.
Motivación Financiera (Cybercrime)	3	FIN7, UNC5736, UNC5537	**Alto:** Riesgo de interrupción por extorsión (Ransomware) y robo de activos financieros.
Distribución de Malware (Botnets)	2	UNC3840, UNC2053	**Medio:** Facilitadores de acceso inicial para otros actores más peligrosos.
No Clasificados / Emergentes	2	UNC4515, UNC1543	**Alto:** Grupos con tácticas en evolución dirigidas específicamente a la región.

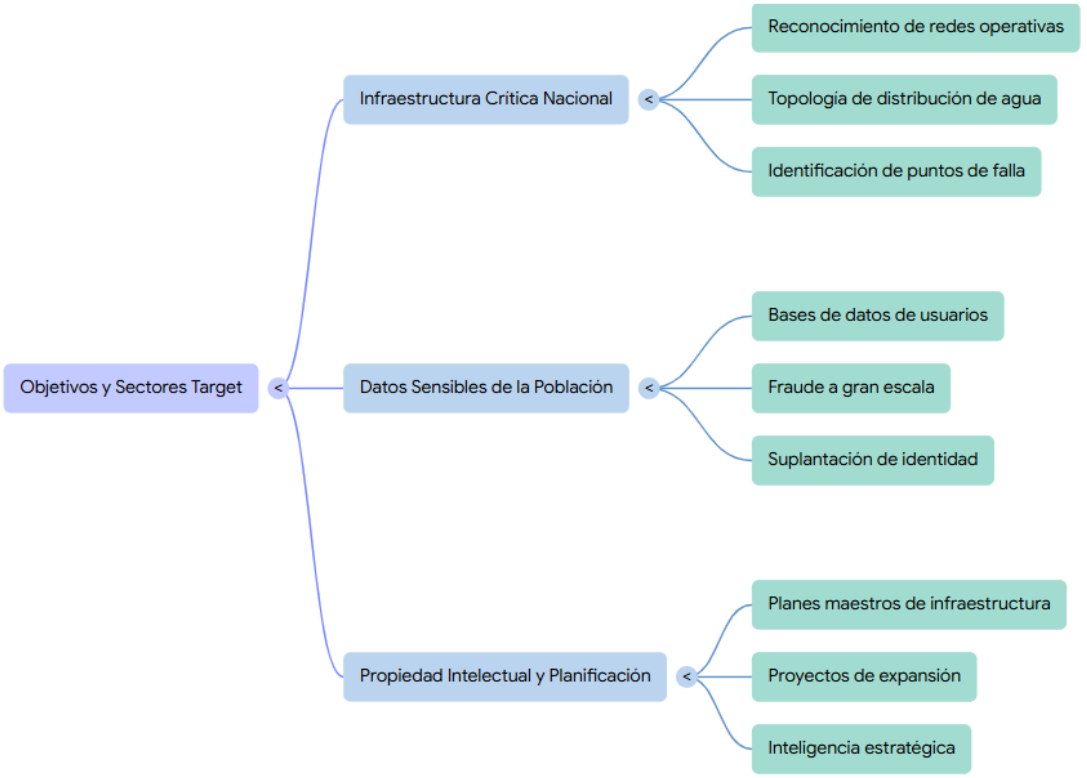
Identificación de Actores Relevantes

La identificación de estos grupos se basa en la correlación de sus tácticas, técnicas y procedimientos (TTPs) con la infraestructura crítica de Colombia. Se destaca la presencia de actores vinculados a operaciones de Estado-nación que poseen un historial documentado de ataques a sistemas de agua en otras geografías, lo que sitúa al sector hídrico colombiano en un nivel de riesgo preventivo elevado frente a posibles acciones de desestabilización.

- ✓ Diversidad de Origen: Los actores identificados provienen de diversas regiones geográficas, lo que indica que el sector no enfrenta una única amenaza, sino un ecosistema de adversarios globalizados.
- ✓ Ciclo de Vida de los Activos: El tiempo promedio entre la modificación de los perfiles de estos actores es de menos de 10 días, lo que demuestra una alta tasa de actualización en sus herramientas y métodos.
- ✓ Nivel de Sofisticación: El 70% de los grupos identificados cuentan con capacidades para desarrollar artefactos personalizados, evitando detecciones genéricas basadas en firmas.

Objetivos y Sectores Target

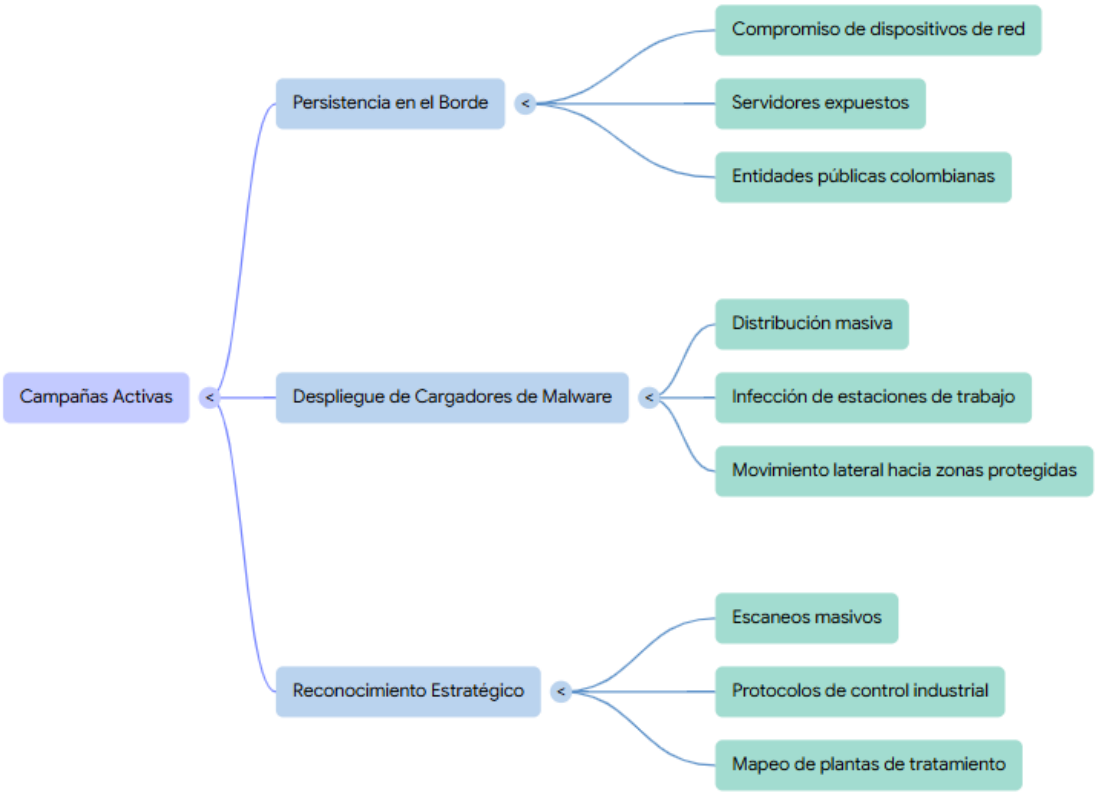
Los adversarios identificados comparten un interés estratégico en sectores que manejan activos físicos y económicos de gran escala. En el contexto colombiano, sus objetivos principales son:



- ✓ **Infraestructura Crítica Nacional:** El objetivo primordial es el reconocimiento de redes operativas para entender la topología de distribución del agua y los puntos de falla.
- ✓ **Datos Sensibles de la Población:** Interés en las bases de datos de usuarios para la ejecución de campañas de fraude a gran escala y suplantación de identidad.
- ✓ **Propiedad Intelectual y Planificación:** Acceso a planes maestros de infraestructura y proyectos de expansión del sector para inteligencia estratégica.

Campañas Activas

Se han detectado múltiples campañas de ataque en curso que utilizan los siguientes métodos:



- ✓ Operaciones de Persistencia en el Borde: Campañas enfocadas en el compromiso de dispositivos de red y servidores expuestos de entidades públicas colombianas.
- ✓ Despliegue de Cargadores de Malware: Uso de herramientas de distribución masiva para infectar estaciones de trabajo administrativas y facilitar el movimiento lateral hacia zonas protegidas.
- ✓ Campañas de Reconocimiento Estratégico: Escaneos masivos dirigidos a protocolos de control industrial para mapear la exposición de las plantas de tratamiento en el país.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

Para la estructuración de esta sección, se ha realizado una correlación entre el comportamiento observado de los adversarios identificados y el marco de referencia **MITRE ATT&CK**. Este mapeo permite entender no solo qué están haciendo los atacantes, sino cómo lo ejecutan dentro de la cadena de valor de las organizaciones del sector Agua en Colombia.

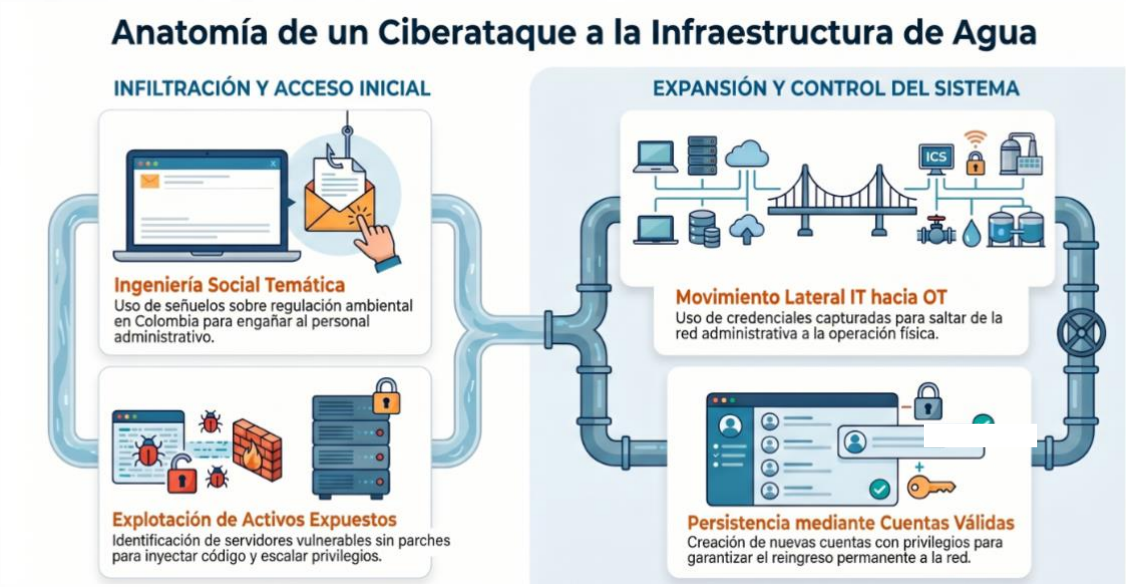
El siguiente análisis detalla las tácticas y técnicas más recurrentes utilizadas por los grupos que operan en el territorio nacional. Dada la naturaleza del sector, los atacantes priorizan la persistencia y el movimiento lateral para alcanzar sistemas que puedan comprometer la continuidad del servicio o la integridad de los datos operativos.

ID	Táctica	Técnica	Justificación para el Sector Agua
T1566	Acceso Inicial	Phishing	Uso de correos dirigidos a empleados administrativos con señuelos sobre regulación hídrica.
T1190	Acceso Inicial	Exploit Public-Facing Application	Explotación de vulnerabilidades en portales de atención al ciudadano o interfaces de gestión técnica.
T1059	Ejecución	Command and Scripting Interpreter	Uso de scripts (Python/PowerShell) para automatizar la recolección de datos en servidores locales.
T1133	Persistencia	External Remote Services	Aprovechamiento de conexiones VPN o RDP mal configuradas para mantener el acceso a la red interna.
T1078	Descubrimiento	Valid Accounts	Uso de credenciales legítimas obtenidas mediante filtraciones previas para operar sin levantar sospechas.
T1083	Descubrimiento	File and Directory Discovery	Búsqueda de planos maestros, manuales de operación de plantas y bases de datos de usuarios.
T1021	Movimiento Lateral	Remote Services	Desplazamiento desde la red administrativa hacia la red de control industrial (OT).
T1005	Recolección	Data from Local System	Extracción de información crítica almacenada en estaciones de trabajo de ingenieros y operadores.
T1041	Exfiltración	Exfiltration Over C2 Channel	Envío de información estratégica hacia servidores externos controlados por los atacantes.
T1486	Impacto	Data Encrypted for Impact	Cifrado de sistemas críticos para exigir rescates, afectando la facturación o la gestión operativa.

Cadenas de Ataque Observadas

Las cadenas de ataque (o *Kill Chains*) identificadas para el sector Agua en Colombia muestran un enfoque altamente estructurado. Los atacantes no actúan de forma aleatoria; siguen un proceso que comienza con el reconocimiento pasivo de la infraestructura y culmina en la exfiltración de datos o el secuestro de sistemas. Esta progresión evidencia que el sector está bajo la mira de actores que comprenden el valor estratégico de la continuidad del suministro hídrico.

Cadenas de ataque:



- ✓ Compromiso mediante Ingeniería Social: Los atacantes utilizan señuelos temáticos relacionados con la regulación ambiental en Colombia para engañar a personal administrativo. Una vez que el usuario interactúa con un archivo malicioso, se establece una conexión inversa hacia la infraestructura del atacante.

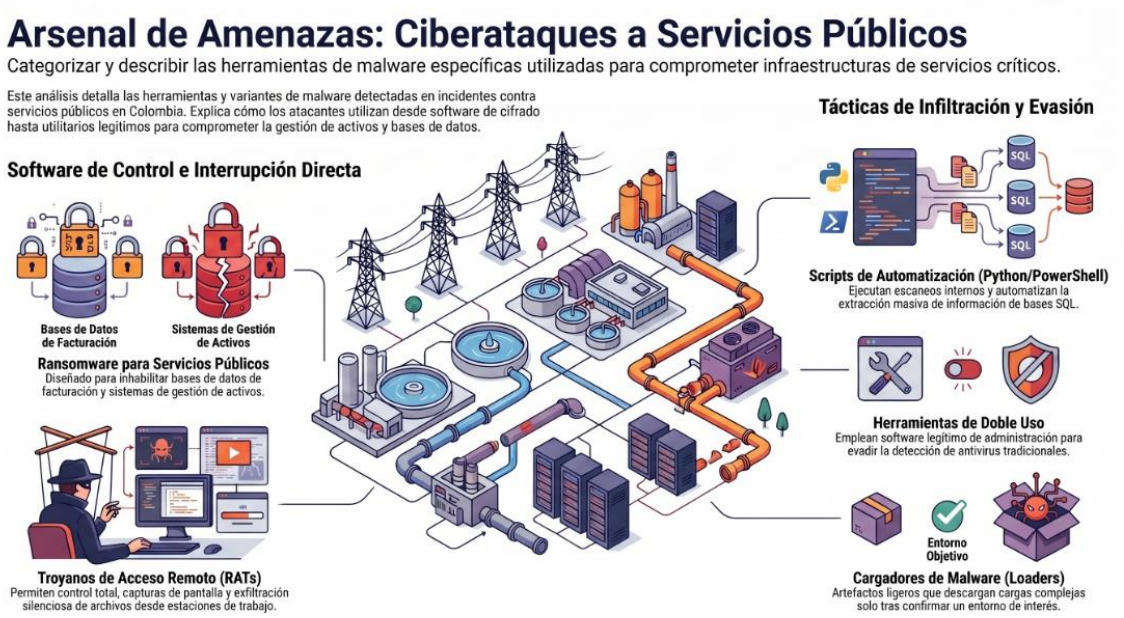
- ✓ Explotación de Activos Expuestos: Identificación de servidores o aplicaciones web con vulnerabilidades conocidas y sin parches de seguridad. Los atacantes inyectan código para ganar acceso inicial y luego escalan privilegios para controlar el servidor afectado.

- ✓ Movimiento Lateral OT/IT: Tras comprometer la red administrativa (IT), los actores de amenaza buscan puentes de comunicación hacia la red de control industrial (OT). Utilizan credenciales legítimas capturadas para saltar hacia sistemas que gestionan la operación física del agua.

- ✓ Persistencia mediante Cuentas Válidas: Una vez dentro, los atacantes crean nuevas cuentas de usuario o comprometen cuentas existentes con privilegios

elevados. Esto les permite reingresar a la red incluso si el vector de entrada original es cerrado.

Herramientas y Malware Específico



- ✓ **Software de Extorsión (Ransomware):** Variantes de cifrado detectadas en incidentes de servicios públicos en Colombia, diseñadas para inhabilitar bases de datos de facturación y sistemas de gestión de activos.

- ✓ **Troyanos de Acceso Remoto (RATs):** Herramientas que permiten a los atacantes tomar el control total de una estación de trabajo, capturar pantallas, registrar pulsaciones de teclas y extraer archivos de forma silenciosa.

- ✓ **Scripts de Automatización (Python/PowerShell):** Uso de scripts personalizados para realizar escaneos internos de red, identificar bases de datos SQL y automatizar la exfiltración de grandes volúmenes de información.

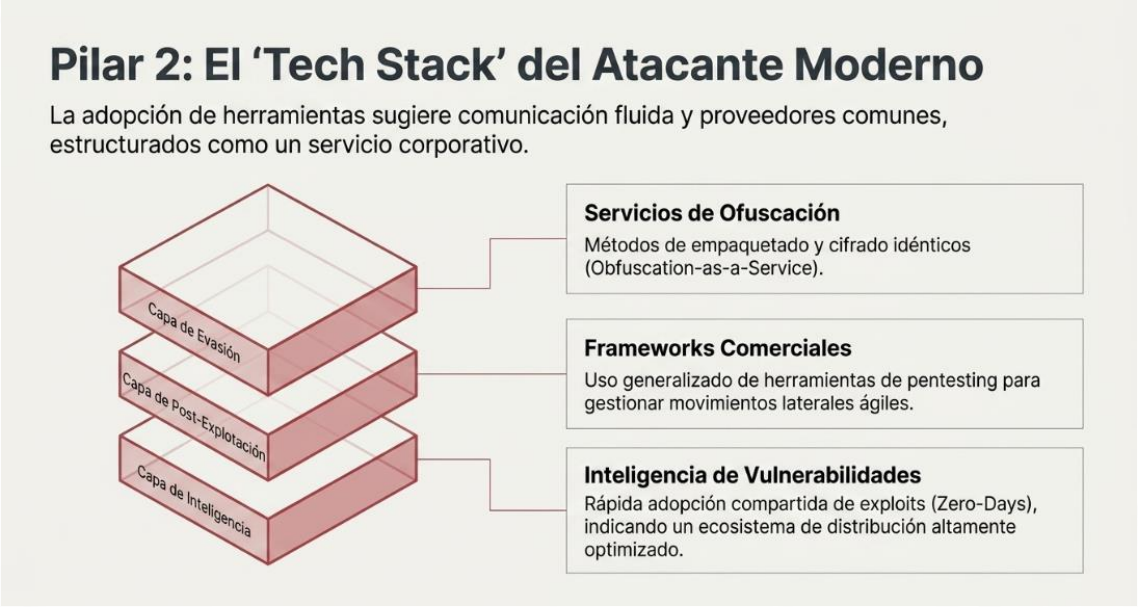
- ✓ **Herramientas de Doble Uso:** Empleo de utilitarios legítimos de administración de sistemas (como herramientas de red y gestión remota) para realizar actividades maliciosas, lo que dificulta la detección por parte de antivirus tradicionales.

- ✓ **Cargadores de Malware (Loaders):** Artefactos ligeros cuya única función es descargar y ejecutar cargas útiles más pesadas y complejas una vez que confirman que se encuentran en un entorno de interés.

CORRELACIÓN ENTRE ACTORES Y GRUPOS

El análisis de inteligencia sugiere que los actores de amenaza no operan de forma aislada. Existe una superposición significativa en el uso de recursos tecnológicos y metodologías de ataque entre grupos de motivación política (APT) y grupos de cibercrimen organizado. Esta correlación indica la existencia de un mercado de servicios ilícitos donde los accesos iniciales a infraestructuras críticas en Colombia son vendidos o intercambiados, permitiendo que actores con objetivos de sabotaje aprovechen las brechas abiertas por delincuentes financieros.

Infraestructura Compartida

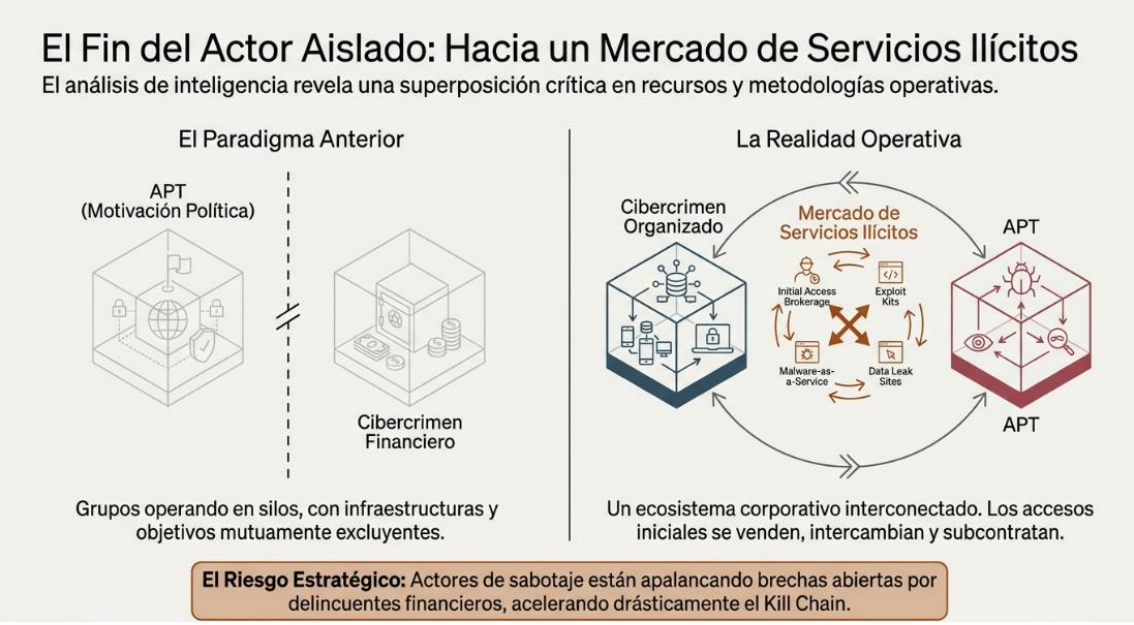


- ✓ **Servidores de Salto (Jump Hosts):** Se ha identificado el uso recurrente de los mismos proveedores de servicios de internet y centros de datos para alojar nodos de comando y control (C2) por parte de diferentes grupos.

- ✓ **Redes de Proxy Volátiles:** El uso de infraestructuras de red comprometidas en la región para enmascarar el origen real de los ataques, dificultando la atribución y el bloqueo geográfico.

- ✓ **Sistemas de Registro de Dominios:** Preferencia por registradores que ofrecen anonimato, donde se han detectado dominios maliciosos de distintos actores creados bajo los mismos patrones de nomenclatura.

Herramientas y TTPs Comunes

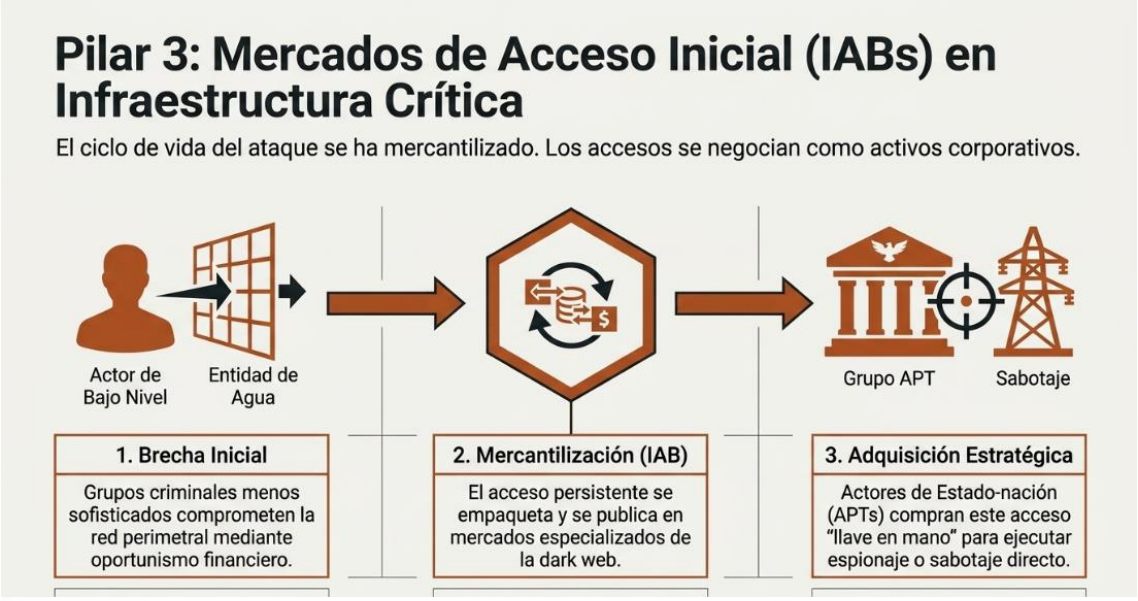


- ✓ **Uso de Frameworks de Post-Explotación:** Múltiples grupos emplean versiones modificadas de herramientas de pruebas de penetración comerciales para gestionar sus movimientos laterales dentro de las redes colombianas.

- ✓ **Técnicas de Ofuscación Similares:** El empleo de métodos de empaquetado y cifrado de código idénticos, lo que sugiere el uso de los mismos "servicios de ofuscación" disponibles en foros especializados de la dark web.

- ✓ **Aprovechamiento de Vulnerabilidades Zero-Day:** La rapidez con la que diferentes actores adoptan nuevos exploits indica una comunicación fluida o una base de proveedores de inteligencia común.

Posibles Colaboraciones o Vínculos



- ✓ **Mercados de Acceso Inicial (IABs):** Grupos menos sofisticados comprometen la red de una entidad de agua y venden ese acceso a grupos APT interesados en el espionaje o sabotaje estratégico.

- ✓ **Subcontratación de Capacidades:** Actores de Estado-nación que utilizan la infraestructura de grupos criminales para llevar a cabo operaciones de negación de servicio (DDoS) o despliegue de software extorsivo como maniobra de distracción.

- ✓ **Intercambio de Metodologías:** La adopción casi simultánea de nuevas tácticas de evasión de defensas locales en Colombia por parte de actores geográficamente distantes apunta a una coordinación técnica o ideológica.

Visualización de Relaciones

El ecosistema de amenazas no es una estructura lineal, sino una red compleja de interdependencias. Mediante el análisis de telemetría y reportes de inteligencia, se ha logrado mapear cómo actores con objetivos aparentemente disímiles convergen en el uso de recursos técnicos. Esta visualización permite identificar nodos críticos de infraestructura que, al ser bloqueados, pueden degradar la capacidad operativa de

múltiples grupos de ataque simultáneamente, mejorando la eficiencia de la defensa proactiva.

Relaciones directas documentadas:

- ✓ Vínculos APT44 - UNC3559: Se han documentado solapamientos en las fases de reconocimiento, donde ambos grupos han mostrado interés en los mismos activos de control industrial (ICS) dentro de la región, sugiriendo una posible transferencia de objetivos estratégicos.

- ✓ Conexión FIN7 - Operadores de Ransomware: Existe una relación directa entre el acceso inicial obtenido por este grupo y el despliegue posterior de cargas útiles extorsivas, funcionando como un facilitador de entrada para campañas de alto impacto financiero.

- ✓ Sinergia APT34 y Campañas de Phishing: Este actor utiliza infraestructuras de apoyo que han sido vinculadas a campañas masivas de recolección de credenciales, aprovechando el volumen de datos filtrados para seleccionar sus objetivos de mayor valor.

Relaciones por infraestructura compartida

- ✓ Uso de Botnets Transversales: Los grupos UNC3840 y UNC2053 comparten nodos de red que sirven como etapa de salto inicial para la distribución de malware de otros actores con mayores capacidades técnicas.

- ✓ Certificados Digitales Comprometidos: Se ha identificado el uso de certificados de firma de código emitidos por las mismas entidades fraudulentas, utilizados tanto por grupos de ciberespionaje como por desarrolladores de malware financiero.

- ✓ Servidores de Comando y Control (C2) en la Región: Múltiples actores de la serie UNC (Uncategorized) han sido detectados operando desde la misma infraestructura de red local en Colombia, lo que indica un aprovechamiento de la latencia y la confianza en proveedores regionales.

Relaciones por herramientas comunes

- ✓ **Adopción de Frameworks de Post-Explotación:** La mayoría de los actores identificados (especialmente grupos de las series **UNC**) utilizan versiones personalizadas de herramientas de pruebas de penetración comerciales para el movimiento lateral y la persistencia.

- ✓ **Scripts de Reconocimiento Estandarizados:** El uso de scripts de automatización en Python y PowerShell con estructuras de código casi idénticas sugiere que los atacantes acceden a las mismas librerías de herramientas en el mercado negro.

- ✓ **Mecanismos de Evasión de EDR:** Se observa una correlación en las técnicas de "By-passing" de soluciones de seguridad de punto final, lo que apunta a un conocimiento compartido sobre las debilidades de las herramientas de defensa desplegadas en Colombia.

Nodos aislados o con baja correlación (por ahora):

- ✓ **UNC4515:** Este actor muestra patrones de comportamiento y protocolos de comunicación únicos, lo que dificulta su vinculación con otros grupos conocidos y sugiere una operación altamente independiente o emergente.

- ✓ **APT19:** Aunque mantiene actividad, sus TTPs se mantienen en un nicho muy específico de espionaje, con poca interacción con la infraestructura de grupos dedicados al cibercrimen financiero.

- ✓ **UNC5736:** Debido a su enfoque en campañas de impacto rápido y cambio constante de activos, la correlación de su infraestructura a largo plazo sigue siendo baja, manteniéndose como un nodo volátil en el mapa de amenazas.

RECOMENDACIONES ESTRATÉGICAS

La protección de la infraestructura de agua en Colombia requiere un enfoque integral que trascienda la simple implementación de herramientas. Las recomendaciones estratégicas aquí descritas están orientadas a cerrar las brechas explotadas por grupos de persistencia avanzada y actores financieros, priorizando la visibilidad sobre los sistemas de control y la protección del dato ciudadano. La estrategia se basa en un

modelo de defensa en profundidad, donde la prevención se complementa con una detección ágil y una capacidad de respuesta probada.

Recomendaciones de Mitigación Técnica

Acciones orientadas a reducir la superficie de ataque y endurecer los activos tecnológicos frente a intentos de explotación.

- **Implementación de Micro-segmentación:** Aislar los entornos de control operativo (OT) de las redes administrativas para impedir el movimiento lateral de los atacantes.
- **Gestión Centralizada de Vulnerabilidades:** Establecer un ciclo de parcheo prioritario para aplicaciones expuestas a internet, eliminando los vectores de entrada detectados en el histórico de incidentes.
- **Robustecimiento de Identidades:** Desplegar autenticación de múltiples factores (MFA) en todos los servicios de acceso remoto y cuentas con privilegios elevados.

Recomendaciones de Detección y Monitoreo

Enfoque proactivo para identificar la presencia de adversarios antes de que logren ejecutar sus acciones finales.

- **Monitoreo de Comportamiento en Redes Industriales:** Implementar sensores de red capaces de detectar anomalías en protocolos específicos de gestión de agua y saneamiento.
- **Integración de Inteligencia de Amenazas:** Automatizar el bloqueo de los Indicadores de Compromiso (IoCs) identificados (IPs, dominios y hashes) en las soluciones de seguridad perimetral.
- **Auditoría de Logs de Acceso:** Supervisar en tiempo real los inicios de sesión fuera de horarios laborales o desde geografías no autorizadas.

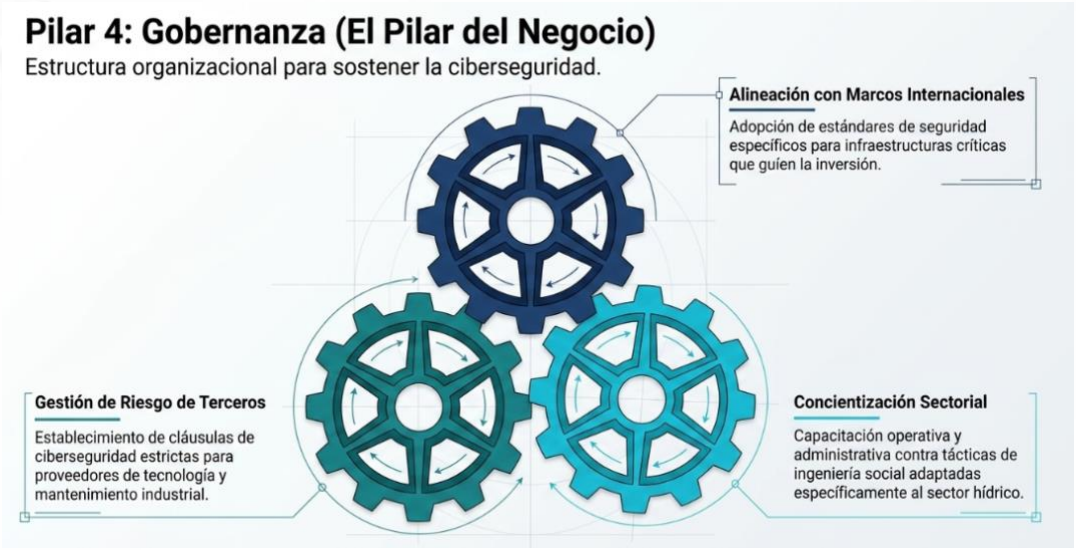
Recomendaciones de Resiliencia Operativa

Capacidad de la organización para mantener la prestación del servicio vital incluso bajo condiciones de compromiso digital.

- **Pruebas de Continuidad de Sistemas Críticos:** Realizar simulacros de operación manual de plantas de tratamiento y bombeo en caso de caída total de los sistemas digitales.
- **Estrategia de Respaldos "Air-Gapped":** Mantener copias de seguridad de datos críticos fuera de línea o en entornos inmutables para mitigar el impacto de ataques de cifrado.
- **Redundancia de Canales de Comunicación:** Garantizar medios alternos de coordinación interna y con autoridades ante incidentes que afecten la red corporativa.

Recomendaciones de Gobernanza

Estructura organizacional y normativa necesaria para sostener la ciberseguridad como un pilar del negocio.



- **Alineación con Marcos Internacionales:** Adoptar estándares de seguridad específicos para infraestructuras críticas que guíen la inversión y el cumplimiento regulatorio.
- **Programas de Concientización Sectorial:** Capacitar al personal operativo y administrativo en la identificación de tácticas de ingeniería social específicas para el sector hídrico.
- **Gestión de Riesgo de Terceros:** Establecer cláusulas de ciberseguridad estrictas para proveedores de tecnología y servicios de mantenimiento industrial.

Preparación ante Incidentes

Fortalecimiento de la capacidad de respuesta para minimizar el tiempo de recuperación.

- **Actualización del Plan de Respuesta a Incidentes (IRP):** Integrar playbooks específicos para ataques de denegación de servicio y compromiso de sistemas de control.
- **Establecimiento de Acuerdos con Aliados:** Definir protocolos de intercambio de información con otros prestadores de servicios públicos y organismos nacionales de ciberseguridad.
- **Ejercicios de Mesa (Tabletop):** Involucrar a la alta dirección en simulacros de crisis para agilizar la toma de decisiones estratégicas durante un evento real.

Acciones Inmediatas (Quick Wins)

Medidas de ejecución rápida que generan un impacto positivo inmediato en la seguridad.

- **Cierre de Puertos de Gestión Expuestos:** Inhabilitar interfaces de administración (como RDP o SSH) que sean visibles directamente desde internet.
- **Revisión de Cuentas de Ex-empleados:** Realizar un purgado inmediato de credenciales activas que ya no tengan una función operativa justificada.
- **Bloqueo de Dominios Maliciosos Recientes:** Aplicar en las puertas de enlace de correo y navegación los indicadores de alta confianza reportados en las últimas 72 horas.

CONCLUSIONES

✓ **Elevada Exposición de Infraestructura Crítica:** El sector presenta una superficie de ataque ampliada debido a la convergencia entre las redes administrativas (IT) y los sistemas de control operativo (OT). Esta interconectividad, sin la debida segregación, posiciona a las plantas de tratamiento y sistemas de bombeo como objetivos vulnerables ante posibles actos de sabotaje digital.

✓ **Predominio de Actores con Motivación Mixta:** Se identifica una coexistencia de grupos de persistencia avanzada (APT) con fines de espionaje estratégico y grupos de cibercrimen financiero. Esta dualidad indica que el sector no solo corre

riesgos de interrupción operativa, sino también de extorsión mediante el cifrado de datos críticos de facturación y usuarios.

- ✓ **Vulnerabilidad Crítica en Aplicaciones y Activos Expuestos:** El historial de incidentes revela que el compromiso de aplicaciones y la falta de gestión de parches en sistemas vulnerables son los vectores de entrada más exitosos. La recurrencia de estos eventos sugiere que las defensas actuales están siendo superadas por técnicas de explotación de vulnerabilidades conocidas.

- ✓ **Uso de Colombia como Nodo de Interés Regional:** Los actores de amenaza están utilizando infraestructura local y ajustando sus tácticas (TTPs) específicamente para el entorno colombiano. Esto demuestra que las campañas no son genéricas, sino que existe un proceso de reconocimiento y adaptación para evadir los controles de seguridad de las entidades nacionales.

- ✓ **Correlación y Colaboración entre Grupos de Amenaza:** Existe una clara interdependencia en el ecosistema de atacantes, donde se comparte infraestructura de comando y control y herramientas de intrusión. Esta colaboración facilita que actores con capacidades limitadas logren compromisos de alto impacto al utilizar accesos o utilitarios desarrollados por grupos más sofisticados.

- ✓ **Necesidad de un Modelo de Resiliencia Proactiva:** La ciberseguridad en el sector debe evolucionar de un enfoque puramente reactivo a uno basado en la resiliencia operativa. Dado que el riesgo de compromiso es latente y persistente, la capacidad de mantener la prestación del servicio vital mediante operaciones manuales o sistemas redundantes es tan crítica como la protección perimetral misma.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- ✓ **Indicador de Compromiso (IoC):** Registro técnico de datos que evidencia, con un alto nivel de certeza, una intrusión activa o pasada en una red corporativa o en un dispositivo tecnológico de la organización.

- ✓ **Tácticas, Técnicas y Procedimientos (TTPs):** Patrones metodológicos de comportamiento y uso de la tecnología que describen cómo actúa un adversario o grupo de amenaza durante el ciclo de vida de un ciberataque.

- ✓ **Persistencia:** Métodos empleados por un adversario para mantener un acceso constante e ininterrumpido dentro de un entorno informático, permitiéndole reingresar incluso ante reinicios de servidores o reajustes de contraseñas de red.

- ✓ **Movimiento Lateral:** Proceso en el cual un atacante, tras obtener acceso inicial a un sistema informático, navega a través de la infraestructura interna buscando ganar privilegios elevados y llegar a activos de mayor criticidad.

- ✓ **Actor de Amenaza Persistente Avanzada (APT):** Grupo organizado y altamente capacitado que ejecuta operaciones digitales dirigidas y persistentes en el tiempo, a menudo motivado por espionaje estratégico y respaldado por amplios recursos de infraestructura.

- ✓ **Ingeniería Social:** Manipulación psicológica dirigida a colaboradores de una organización para engañarlos y conseguir que ejecuten código malicioso, descarguen archivos infectados o revelen credenciales de acceso estratégicas.

- ✓ **Exfiltración de Datos:** Transferencia de datos, documentos y planos confidenciales desde el interior de la infraestructura tecnológica de la víctima hacia servidores de almacenamiento externos controlados por el atacante.

- ✓ **Campaña de Amenaza:** Conjunto coordinado de operaciones cibernéticas hostiles que siguen objetivos comunes de reconocimiento, infiltración o impacto contra sectores específicos en un marco geográfico y temporal definido.

Infraestructura y Redes

- ✓ **Sistemas de Control Industrial (ICS):** Dispositivos físicos, software e infraestructura de telecomunicaciones encargados de automatizar, monitorear y supervisar los procesos de la infraestructura operativa real (como la presión del agua, compuertas y químicos de potabilización).

- ✓ **SCADA (Supervisory Control and Data Acquisition):** Arquitectura informática destinada a la supervisión operativa y adquisición de datos en tiempo real de plantas físicas remotas y procesos de distribución de alto impacto.

- ✓ **Tecnología de la Operación (OT):** Entorno de hardware y software de control directo dedicado a gestionar los cambios sobre procesos físicos en la operación industrial, caracterizado por requerir niveles críticos de disponibilidad en tiempo real.

- ✓ **Tecnología de la Información (IT):** Infraestructura tecnológica que compone el soporte administrativo y financiero de una organización, encargada de la gestión de bases de datos de clientes, facturación, portales web corporativos y servidores de correo.

- ✓ **Segregación de Redes:** Medida técnica y arquitectónica que divide los activos de red de una organización en diferentes zonas aisladas de confianza, impidiendo que el compromiso de sistemas administrativos (IT) afecte a los sistemas industriales (OT).

- ✓ **Servicio de Acceso Remoto Externo:** Puntos de conexión virtuales que habilitan a contratistas, técnicos externos o ingenieros de soporte de la empresa a ingresar de manera controlada y segura a la red interna desde fuera de la red local.

- ✓ **Servidor de Comando y Control (C2):** Infraestructura externa operada por atacantes que envía órdenes automáticas a los archivos de software malicioso implantados en la red víctima, recibiendo además los datos recolectados por estos.

- ✓ **Dispositivos de Borde:** Equipos perimetrales de la infraestructura corporativa que interactúan directamente con el tráfico de internet público, tales como firewalls, servidores de correo externos o balanceadores de carga.

Herramientas y Malware

- ✓ **Malware:** Software o código informático hostil desarrollado con la finalidad de interrumpir operaciones de red, recolectar información sensible, alterar bases de datos o evadir controles de seguridad instalados.
- ✓ **Software de Extorsión (Ransomware):** Programa malicioso que tiene la capacidad de cifrar los datos del disco duro de un servidor u ordenador, bloqueando el acceso al sistema corporativo y solicitando un pago para su recuperación.

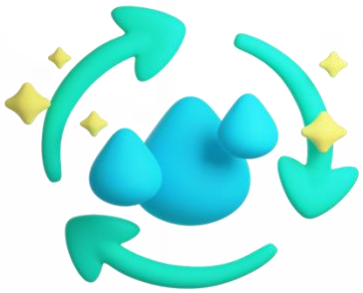
- ✓ **Troyano de Acceso Remoto (RAT):** Código informático dañino que imita funcionalidades de administración remota, permitiendo a los ciberdelincuentes supervisar de manera encubierta la actividad de un equipo infectado y ejecutar comandos a distancia.
- ✓ **Cargador (Loader):** Componente ligero de código que sirve como primer eslabón para evadir defensas perimetrales y que se encarga exclusivamente de descargar la carga útil real del malware desde la web una vez infiltrado el dispositivo.
- ✓ **Scripts de Automatización:** Archivos de código desarrollados en lenguajes de scripting que facilitan la ejecución rápida de tareas repetitivas por parte de los atacantes, como la recolección de configuraciones de red o el mapeo de servidores.
- ✓ **Herramientas de Doble Uso:** Utilitarios comerciales y legítimos de administración del sistema y diagnóstico de redes que son aprovechados por los atacantes con fines hostiles, permitiéndoles eludir la detección por firmas de antivirus tradicionales.
- ✓ **Keylogger:** Software malicioso diseñado para interceptar, registrar y transmitir de forma invisible todas las pulsaciones de teclado del usuario con la intención de capturar contraseñas administrativas y datos bancarios.

Sector

- **Infraestructura Crítica Cibernética:** Instalaciones, redes y sistemas del sector agua cuya interrupción o destrucción tendría un impacto mayor en la salud pública, la seguridad y el orden económico de Colombia.
- **CONPES 3854:** Política Nacional de Seguridad Digital en Colombia que establece los lineamientos para que las entidades públicas y privadas fortalezcan sus capacidades de respuesta ante amenazas cibernéticas.
- **CONPES 3995:** Política Nacional de Confianza y Seguridad Digital que busca elevar la resiliencia de la infraestructura nacional frente a riesgos digitales, promoviendo la cooperación entre el sector público y las empresas de servicios públicos.
- **Ley 142 de 1994 (Ley de Servicios Públicos):** Marco normativo que regula la prestación de servicios públicos domiciliarios en Colombia, incluyendo el agua, y que establece la obligación de garantizar la continuidad y calidad del servicio.
- **Superintendencia de Servicios Públicos Domiciliarios (SSPD):** Organismo encargado de la inspección, vigilancia y control de las empresas del sector, que

supervisa la adecuada gestión de riesgos, incluidos los riesgos tecnológicos que puedan afectar la prestación del servicio hídrico.

- **CSIRT Gobierno / CSIRT Nacional:** Grupos de respuesta a incidentes de seguridad informática encargados de coordinar la gestión de crisis y el intercambio de información técnica sobre amenazas que afecten a las entidades del Estado y sectores estratégicos colombianos.
- **Modelo de Madurez de Seguridad Digital:** Herramienta de evaluación que permite a las empresas prestadoras de servicios de agua medir su nivel de preparación y capacidad técnica para enfrentar ataques digitales de acuerdo con los estándares nacionales.
- **Circular Única de la SSPD:** Conjunto de instrucciones técnicas y normativas donde se especifican los requisitos de reporte de información y gestión de riesgos operativos que las empresas de agua deben cumplir ante el ente regulador.
- **Gestión de Riesgo Operativo:** Proceso obligatorio bajo la normativa colombiana para identificar, evaluar y mitigar posibles fallos en la prestación del servicio derivados de ataques informáticos a los sistemas de control o gestión.



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.

La información contenida en este documento, bajo clasificación TLP:CLEAR - Pública, puede ser utilizada y compartida libremente con fines informativos, técnicos y de prevención, siempre que se cite como fuente al Equipo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT). Uso permitido con atribución. © ColCERT, 2026.

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