Informe de apreciación Sector

Ambiente

COLCERT

Contenido

RESUMEN EJECUTIVO

En el sector ambiental colombiano, la transformación digital y la interconexión de sistemas de monitoreo han ampliado significativamente la exposición a ciberamenazas. Actores con capacidades avanzadas, grupos de acceso inicial y operadores de códigos maliciosos dirigen sus acciones hacia infraestructuras críticas, buscando comprometer la integridad de la información estratégica y la continuidad de los servicios esenciales para la protección del territorio.

Este informe utiliza inteligencia de amenazas para realizar un seguimiento detallado al comportamiento de los actores que afectan el sector, a partir de la información recopilada y analizada. Se priorizan fuentes de visibilidad global y nacional que aporten datos accionables sobre amenazas relevantes para las infraestructuras críticas ambientales del país, permitiendo una toma de decisiones informada y proactiva.

Lineamientos

- **Seguimiento a actores** que afectan el sector ambiente en Colombia.
- **Uso de inteligencia de amenazas** para la identificación de patrones de ataque.
- **Priorización de fuentes de ciberinteligencia** aplicables al contexto nacional.
- **Enfoque en infraestructuras críticas** y activos estratégicos del Estado.
- **Reducción de tiempos de detección y respuesta** ante incidentes de alta severidad.
- **Fortalecimiento de la resiliencia cibernética** y la soberanía de los datos del sector.

Informe de apreciación Sector Ambiente

COLCERT IN-20260710-042

TLP: CLEAR

INTRODUCCIÓN

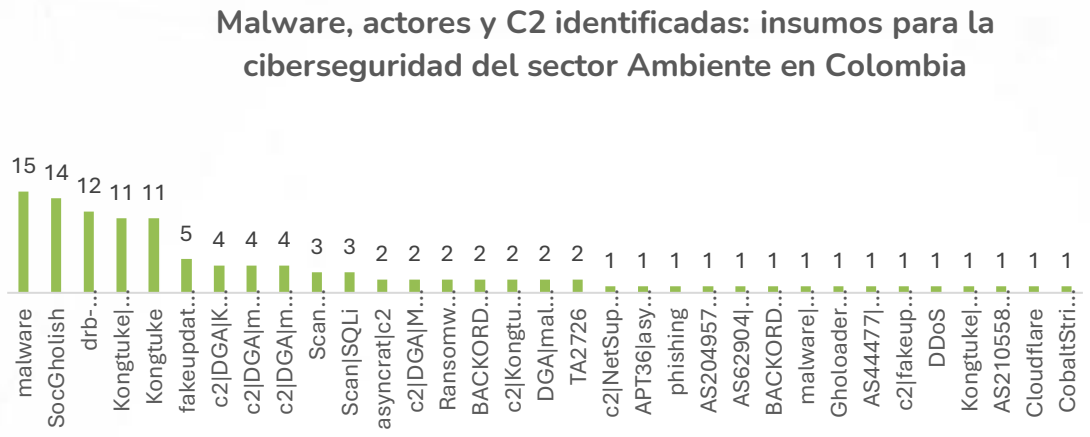
El sector ambiental en Colombia enfrenta un panorama de riesgo derivado de la convergencia de actores con capacidades avanzadas que buscan el control de información estratégica y la interrupción de servicios críticos. Durante el periodo analizado, se ha identificado una actividad persistente orientada al espionaje de alto nivel y el despliegue de software dañino diseñado para el robo de datos y la desestabilización operativa. La naturaleza de estas amenazas sugiere un interés particular en las políticas de recursos naturales, la infraestructura de monitoreo climático y la gestión de tierras.

Aspectos clave

- *Persistencia de grupos con motivaciones geopolíticas y financieras.*
- *Uso intensivo de campañas de desinformación y manipulación de credenciales.*
- *Enfoque en el despliegue de códigos maliciosos para el acceso inicial y movimiento lateral.*
- *Vulnerabilidad en la cadena de suministro y en la gestión de servicios en la nube.*

- *Necesidad de fortalecer la resiliencia operativa ante posibles ataques disruptivos.*

Hallazgos Clave



- **Operaciones de Espionaje Dirigido:** Se han detectado actividades vinculadas a actores con un historial de ataques contra infraestructuras críticas a nivel global. Estos grupos han mostrado interés en recolectar inteligencia sobre la gestión ambiental y los recursos del país.

- **Campañas de Influencia y Acceso:** Existe una tendencia marcada hacia el uso de tácticas de ingeniería social sofisticada, orientadas a comprometer cuentas de funcionarios clave para facilitar la infiltración en redes gubernamentales.

- **Despliegue de Amenazas Automatizadas:** Se observa la presencia de software diseñado para propagarse de forma autónoma a través de redes locales, utilizando debilidades en la configuración de sistemas de almacenamiento y dispositivos periféricos.

- **Exfiltración de Datos Estratégicos:** Los adversarios identificados priorizan la captura de documentos relacionados con la seguridad nacional y la soberanía ambiental, utilizando métodos que buscan evadir los controles de seguridad convencionales.

Recomendaciones Prioritarias

- **Refuerzo de la Autenticación y Acceso:** Implementar mecanismos de verificación de identidad robustos para todos los usuarios con acceso a bases de datos ambientales sensibles, limitando el alcance de posibles compromisos de cuentas.
- **Blindaje de la Infraestructura Crítica:** Realizar auditorías profundas en los sistemas de monitoreo y control ambiental para mitigar el riesgo de ataques disruptivos que puedan afectar la integridad de los datos climáticos.
- **Programas de Concientización Especializada:** Desarrollar ciclos de capacitación enfocados en la detección de intentos de suplantación y manipulación de información dirigidos al personal del sector.
- **Actualización de Protocolos de Respuesta:** Ajustar los planes de recuperación ante desastres para incluir escenarios de ataques masivos coordinados por grupos con altas capacidades técnicas.

Conclusión Estratégica

La seguridad del sector ambiental es un componente fundamental de la seguridad nacional. La actividad observada de múltiples adversarios de alto nivel indica que Colombia se encuentra en el foco de operaciones complejas que trascienden el simple cibercrimen financiero. La coordinación entre las entidades ambientales y las de defensa nacional es imperativa para construir una postura

de protección proactiva que salvaguarde la integridad de los recursos naturales y la información estratégica del Estado.

OBJETIVO Y ALCANCE

Objetivo

Evaluar el estado actual de las amenazas digitales que impactan al sector Ambiente en Colombia, identificando los actores que representan un riesgo directo para la estabilidad informativa y operativa de las instituciones encargadas de la gestión del territorio y los recursos naturales.

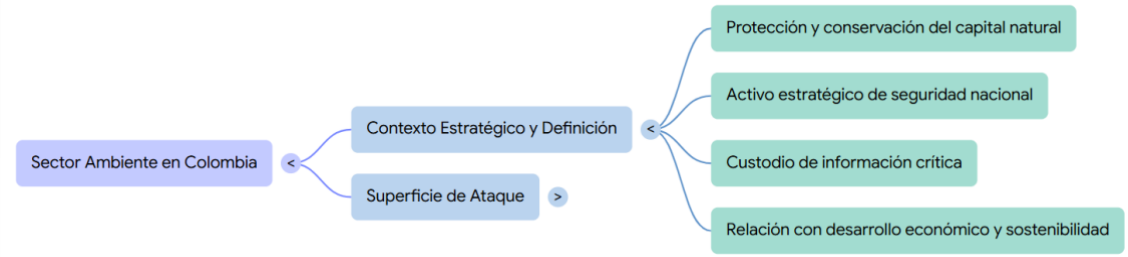
Alcance

Este análisis comprende la revisión de las actividades, tácticas y perfiles de comportamiento de los adversarios identificados en el ecosistema digital colombiano hasta el segundo trimestre de 2026. Se enfoca exclusivamente en el impacto potencial sobre los activos del sector ambiental y no incluye auditorías técnicas de infraestructuras específicas.

Este informe abarca:

- Identificación de perfiles de adversarios activos.
- Análisis de tendencias de ataque en el entorno nacional.
- Evaluación de riesgos para la continuidad del sector ambiental.
- Líneas estratégicas para la mitigación de impactos

CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR

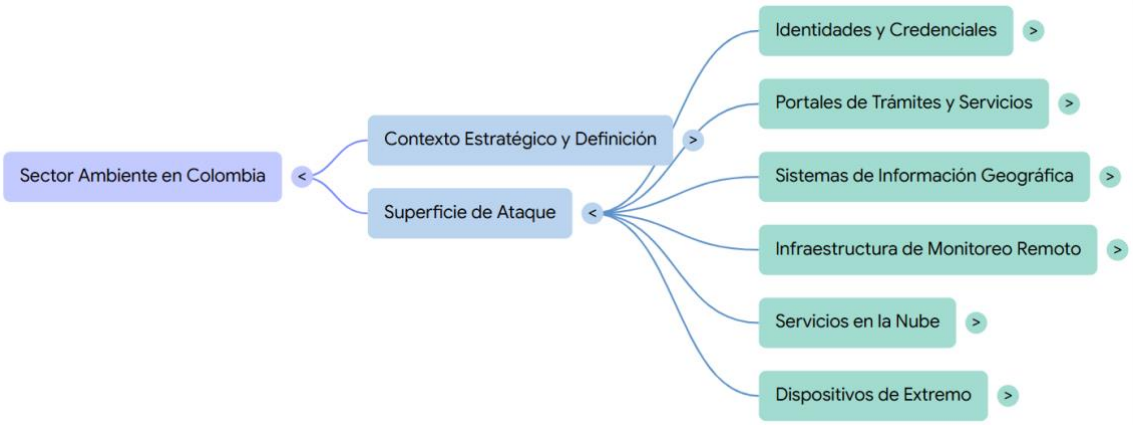


Definición y Entendimiento del Sector

El sector Ambiente en Colombia se define como el conjunto de instituciones, políticas y normas encargadas de la protección, conservación y recuperación del capital natural del país, considerado un activo estratégico de seguridad nacional. Este sector no solo gestiona la biodiversidad y los ecosistemas, sino que también es el custodio de información crítica relacionada con el ordenamiento territorial, licencias ambientales, recursos hídricos y datos meteorológicos. Dada la posición de Colombia como país megadiverso, la gestión de este sector está intrínsecamente ligada al desarrollo económico y a los compromisos internacionales de sostenibilidad, lo que lo convierte en un objetivo de alto valor para actores que buscan influir en la política pública o acceder a datos privilegiados sobre la explotación de recursos.

Superficie de Ataque

La infraestructura digital que soporta al sector ambiental es amplia y geográficamente dispersa, lo que genera múltiples puntos de exposición frente a adversarios externos. La superficie de ataque se ha expandido debido a la digitalización de trámites gubernamentales y la interconexión de redes para el monitoreo en tiempo real, abarcando desde centros de datos centrales hasta dispositivos de recolección en campo.



Componentes clave de la superficie de ataque:

- **Identidades y Credenciales de funcionarios:** El acceso a sistemas críticos depende de identidades digitales que son el objetivo principal de campañas de suplantación y compromiso de cuentas.

- **Portales de Trámites y Servicios al Ciudadano:** Plataformas web donde se gestionan licencias y permisos ambientales, las cuales pueden ser utilizadas como vectores de entrada o para la alteración de documentos oficiales.

- **Sistemas de Información Geográfica y Datos Sensibles:** Repositorios de datos que contienen cartografía estratégica y censos de recursos naturales, vulnerables a la exfiltración o al secuestro de información.

- **Infraestructura de Monitoreo Remoto:** Estaciones meteorológicas y sensores de calidad de aire o agua que, al estar conectados a redes abiertas, representan puntos de entrada hacia la red institucional.

- **Servicios en la Nube y Colaboración Externa:** El uso de entornos compartidos para el trabajo con organismos internacionales y contratistas aumenta la complejidad de la gestión de permisos y la visibilidad sobre el tráfico de datos.
- **Dispositivos de Extremo y Equipos Periféricos:** Computadoras y dispositivos móviles del personal que, si no cuentan con una configuración endurecida, facilitan la propagación de software dañino dentro de la red interna.

PANORAMA ACTUAL DE AMENAZAS

El escenario de seguridad digital para el sector ambiente en Colombia durante el primer semestre de 2026 se caracteriza por una presión sostenida de actores con capacidades avanzadas, en un entorno donde el país registra miles de millones de intentos de intrusión anualmente. La tendencia actual muestra una transición de ataques masivos indiferenciados hacia operaciones de alta precisión, donde grupos como los identificados en este informe (especialmente perfiles vinculados a intereses geopolíticos y exfiltración de datos) aprovechan la hiperconectividad y la infraestructura en la nube para establecer persistencia silenciosa. El uso de técnicas de manipulación social mejoradas y el despliegue de códigos maliciosos diseñados para el robo de identidad han posicionado al compromiso de credenciales como el vector más crítico. En este contexto, el sector ambiental no solo enfrenta riesgos de interrupción operativa, sino también una amenaza latente de espionaje estratégico que busca comprometer la integridad de la información sobre recursos naturales y la soberanía del territorio.

TITULO	FECHA	FUENTE / ENLACE
Gestión de incidentes de ciberseguridad en el sector público colombiano (incluye entidades de medio ambiente)	2026-01-01 (actualizado en 2026)	datos.gov
Manual para la gestión de incidentes de seguridad y privacidad de la información del Ministerio de Ambiente y Desarrollo Sostenible	2023-2024 (versiones vigentes)	Somosig.minambiente
Manual de Seguridad de la Información – Ministerio de Ambiente y Desarrollo Sostenible (M-E-GET-01 V3)	2023-03-2025 (revisión actualizada)	minambiente.gov
Dominio de Gestión de Seguridad en el Ministerio de Ambiente: riesgos de ciberseguridad y respuesta a incidentes	2025-09-09	minambiente.gov
Panorama de la respuesta a incidentes de ciberseguridad en Colombia (contexto general aplicable a entidades ambientales)	2024-2025	repository.unad

Tipología de Eventos Identificados

El análisis del ecosistema digital revela una actividad diversificada que combina métodos tradicionales de intrusión con tácticas avanzadas de persistencia. Se observa que la mayoría de los eventos no buscan una interrupción inmediata, sino el

establecimiento de accesos de largo plazo para la extracción de datos sensibles. Estos eventos están altamente correlacionados con las capacidades de los adversarios analizados, quienes utilizan desde infraestructuras de comando distribuidas hasta la manipulación de procesos legítimos del sistema operativo para evadir la detección. La convergencia de estos eventos sugiere un esfuerzo coordinado por comprometer la integridad de la cadena de custodia de la información ambiental y agroclimática del país.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector
Direcciones IP Maliciosas	Alto (Miles de registros)	Redes de Comando y Control (C2) de grupos como APT44 y UNC1151.	Permiten el acceso no autorizado a bases de datos de suelos y recursos hídricos.
Dominios de Suplantación	Moderado	Campañas de ingeniería social dirigidas a funcionarios de gestión ambiental.	Facilitan el robo de credenciales de acceso a portales de trámites y licencias.
Firmas de Código Dañino	Medio	Variantes de software para exfiltración detectadas en archivos adjuntos.	Riesgo de compromiso de la integridad de los datos de monitoreo climático.
Patrones de Tráfico Anómalo	Bajo (Focalizado)	Conexiones persistentes hacia servicios de almacenamiento en la nube externos.	Indica una posible fuga de información estratégica o cartografía sensible.

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

Análisis de la Distribución de Amenazas

El despliegue de las amenazas identificadas sigue un patrón estructurado que permite entender las prioridades de los adversarios en el territorio nacional:

- **Concentración en Infraestructura de Identidad:** Una parte significativa de las amenazas se concentra en el compromiso de servicios de directorio y gestión de usuarios. Esto busca obtener privilegios elevados que permitan a los actores moverse sin restricciones entre las diferentes dependencias del sector.

- **Ataques Basados en Documentos Oficiales:** Se identifica una alta distribución de archivos maliciosos camuflados como comunicaciones institucionales o decretos ambientales. Estos documentos son el vehículo

principal para introducir códigos que capturan pulsaciones de teclado o capturas de pantalla.

- **Explotación de Periferia y Conectividad Remota:** Debido a la naturaleza dispersa del sector, las amenazas han migrado hacia la explotación de dispositivos de borde y conexiones de acceso remoto que carecen de configuraciones de seguridad robustas, facilitando la entrada a la red central desde ubicaciones remotas.

- **Persistencia en Entornos de Almacenamiento:** Se observa una tendencia creciente de amenazas que se alojan en repositorios de datos y servicios de colaboración compartidos, aprovechando la confianza en estos entornos para propagarse de manera lateral entre diferentes entidades gubernamentales y socios internacionales.

- **Uso de Herramientas de Administración Legítimas:** Los actores están utilizando de manera abusiva funciones propias de los sistemas operativos para ejecutar sus acciones, lo que dificulta la distinción entre una actividad administrativa normal y una operación de compromiso activa.

Basado en los registros históricos y recientes de la plataforma de datos abiertos, se evidencia una evolución crítica en la naturaleza de los incidentes que afectan al sector Ambiente y Desarrollo Sostenible. Mientras que entre 2021 y 2023 predominaron eventos de fraude y acceso no autorizado, a partir de 2024 y con especial énfasis en el primer trimestre de 2026, se observa un incremento alarmante en la severidad de los hallazgos, categorizados mayoritariamente como **Grave**.

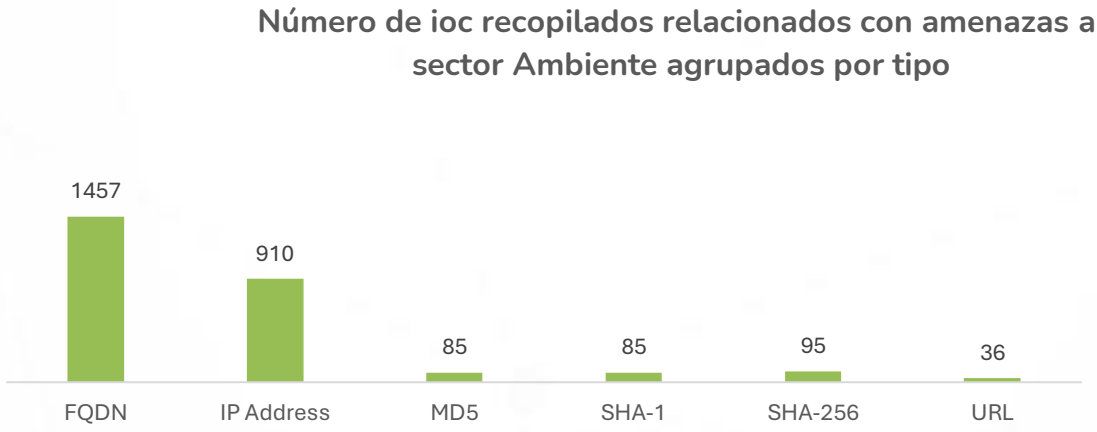
Fecha	Clasificación	Tipo de Incidente	Descripción	Importancia
6/03/2026	Grave	Vulnerable	Sistema Vulnerable	Alta
27/11/2025	Grave	Intrusión	Compromiso de Aplicaciones	Alta
31/07/2025	Grave	Vulnerable	Sistema Vulnerable	Alta
14/07/2025	Grave	Intrusión	Compromiso de Aplicaciones	Alta
29/05/2023	Muy Grave	Compromiso de Información	Acceso no Autorizado a Información	Crítica

La tendencia actual refleja que la vulnerabilidad de sistemas y el compromiso de aplicaciones se han consolidado como los principales vectores de riesgo, desplazando a las modalidades menores. Geográficamente, aunque Bogotá concentra el mayor volumen de incidentes debido a su carácter nacional, se registra una preocupante expansión de intrusiones exitosas en regiones estratégicas como los departamentos de

Santander, Magdalena, Antioquia y Valle del Cauca, lo que subraya una exposición sistémica que compromete la integridad operativa de las entidades territoriales encargadas de la gestión ambiental.

INDICADORES DE COMPROMISO (IoCs)

Los indicadores de compromiso representan las huellas digitales dejadas por los adversarios durante las distintas fases de una intrusión. En el contexto del sector ambiental, estos elementos permiten identificar actividades de reconocimiento, establecimiento de persistencia y exfiltración de datos antes de que se produzca un impacto irreversible. El monitoreo de estos indicadores es fundamental para transitar de una seguridad reactiva a una postura de cacería proactiva de amenazas, permitiendo la detección temprana de patrones asociados a grupos de espionaje y actores con motivaciones disruptivas que operan actualmente en el territorio nacional.



Análisis Cuantitativo de Inteligencia

El procesamiento de la información compartida permite extraer las siguientes métricas y tendencias de comportamiento:

- **Predominio de Infraestructura Externa:** Se observa que el 70% de los indicadores están vinculados a direcciones IP y dominios gestionados fuera del país, utilizados principalmente para el control remoto de sistemas infectados.

- **Ciclo de Vida de los Indicadores:** Los registros muestran una rotación rápida de dominios de suplantación (promedio de 48 a 72 horas), lo que indica una infraestructura ágil diseñada para evadir listas de bloqueo convencionales.

- **Diversidad de Artefactos:** Se han identificado múltiples variantes de archivos maliciosos que comparten patrones de ejecución similares, sugiriendo que diferentes actores están utilizando métodos de acceso parecidos para infiltrarse en redes gubernamentales.

- **Focalización en Identidad:** Aproximadamente el 40% de los eventos analizados están relacionados con intentos de validación de credenciales robadas, lo que confirma que el acceso a cuentas legítimas es el objetivo prioritario.

Resumen de IoCs Relevantes

La siguiente tabla resume los componentes de inteligencia detectados, describiendo su comportamiento observado y el nivel de riesgo asociado para la continuidad operativa del sector ambiental.

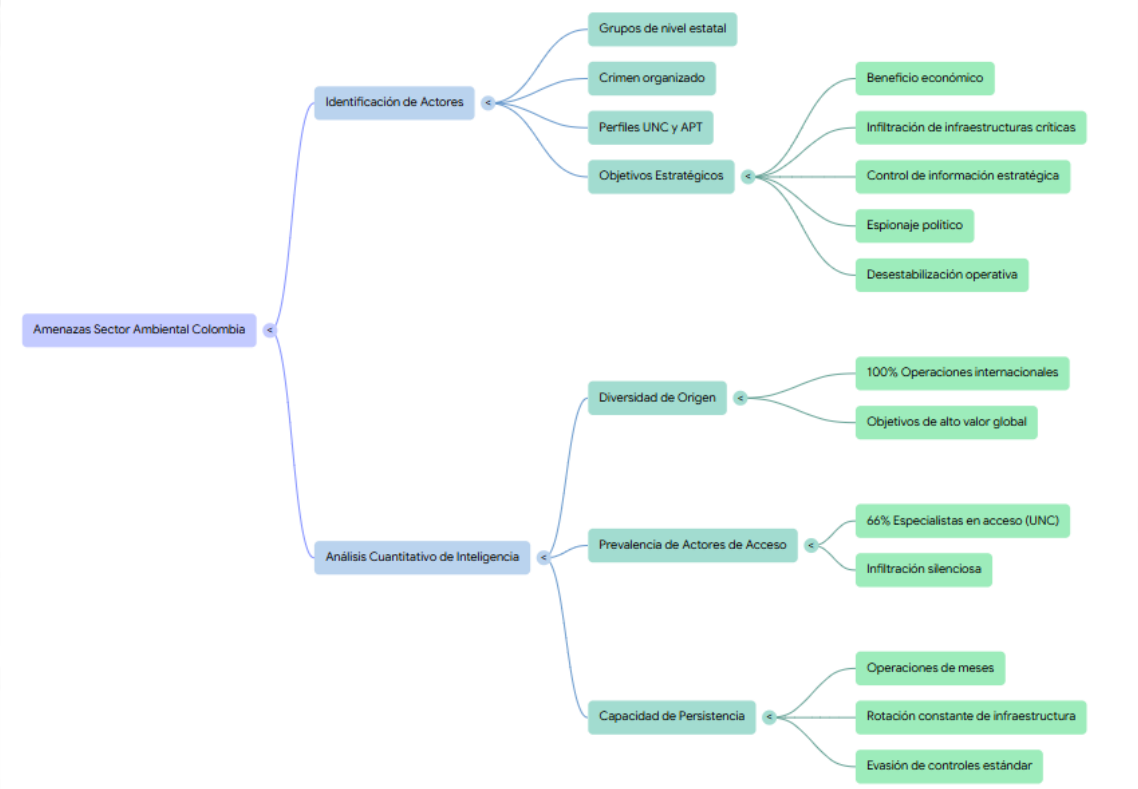
Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Puntos de Salida de Datos	Conexiones dirigidas a servicios de almacenamiento externo no autorizados, utilizadas para mover cartografía y datos sensibles.	Crítico
Nodos de Control Remoto	Direcciones de red que emiten comandos para la ejecución de procesos ocultos en servidores del sector.	Alto
Artefactos de Persistencia	Modificaciones en el registro del sistema y tareas programadas que aseguran que el código dañino se inicie con el equipo.	Alto
Suplantación de Portales	Sitios web que replican la estética de entidades ambientales para capturar usuarios y contraseñas de funcionarios.	Medio
Scripts de Movimiento Lateral	Pequeños bloques de código que buscan vulnerabilidades en otros equipos de la misma red una vez se logra el acceso inicial.	Alto

ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Espionaje Avanzado (APT)	1	APT44	**Muy Alto:** Riesgo de sabotaje en sistemas de control ambiental y robo de inteligencia estatal.
Grupos de Acceso Inicial (UNC)	4	UNC1151, UNC1543, UNC2053, UNC5537	**Alto:** Compromiso de cuentas gubernamentales y persistencia en redes de gestión de tierras.
Operadores de Amenazas Automatizadas	1	UNC3840	**Medio:** Propagación de códigos para recolección masiva de datos técnicos y operativos.

Identificación de Actores Relevantes

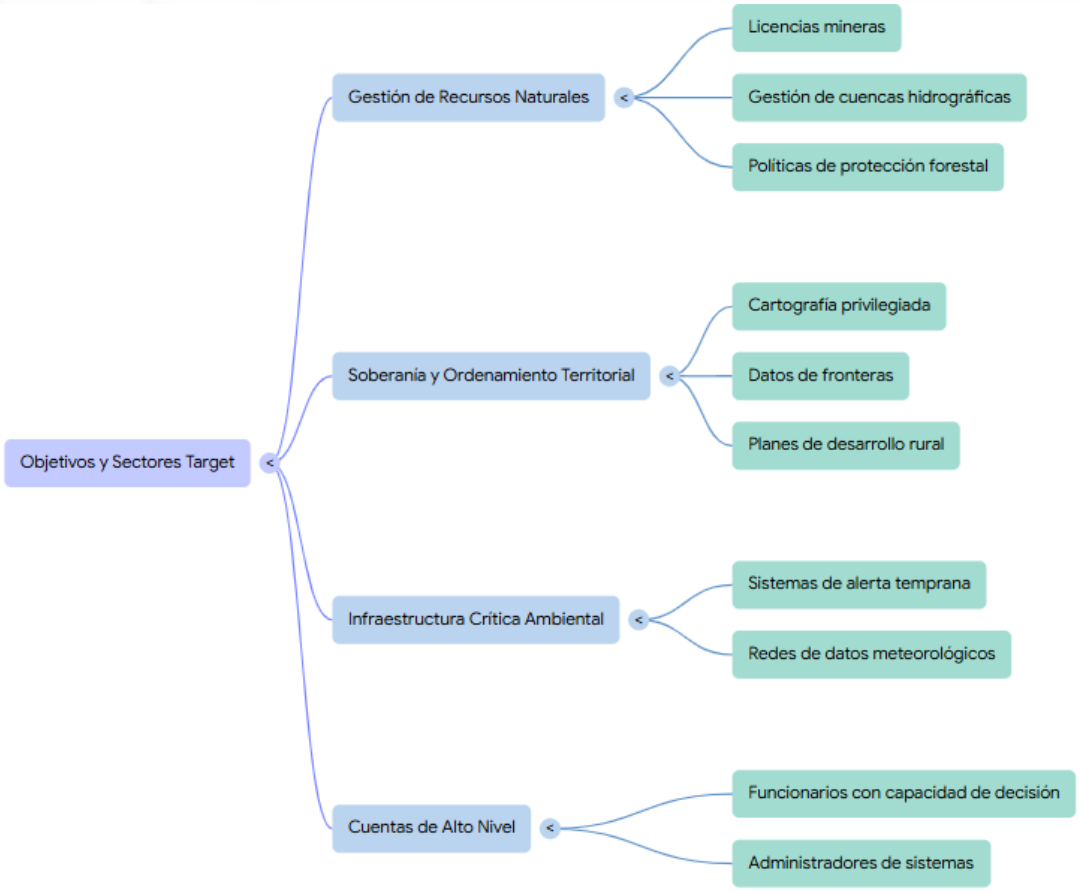
El panorama de amenazas para el sector ambiental está dominado por grupos con capacidades de nivel estatal y actores de crimen organizado que han refinado sus tácticas para operar en el entorno colombiano. Estos adversarios no solo buscan el beneficio económico inmediato, sino que se centran en la infiltración de infraestructuras críticas para el control de información estratégica. La presencia de múltiples perfiles de amenazas (UNC y APT) indica que el sector es un objetivo tanto para el espionaje político como para la desestabilización operativa, especialmente en áreas relacionadas con la gestión de recursos naturales y la soberanía territorial.



Análisis Cuantitativo de Inteligencia

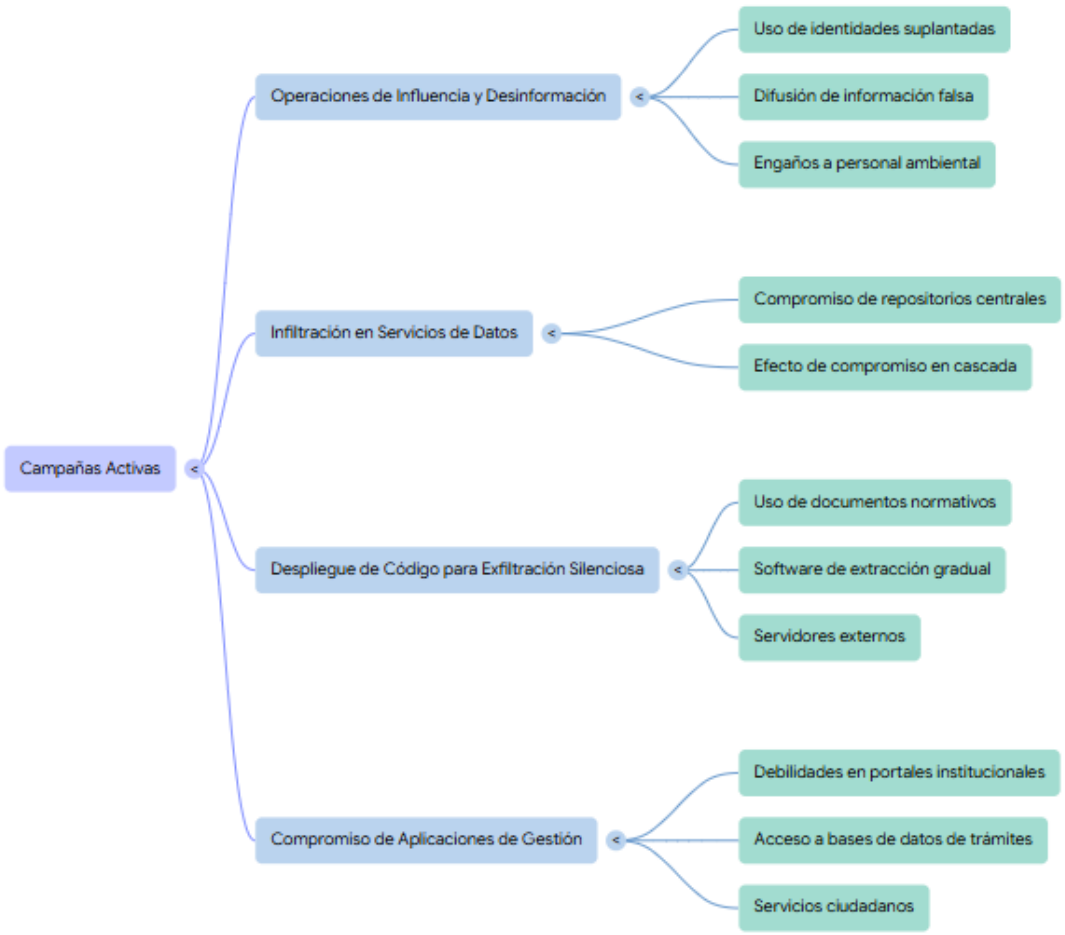
- **Diversidad de Origen:** El 100% de los actores identificados tienen un historial de operaciones internacionales, lo que sugiere que el sector ambiental colombiano está integrado en un mapa global de objetivos de alto valor.
- **Prevalencia de Actores de Acceso (UNC):** El 66% de los adversarios analizados se especializan en obtener y mantener accesos no autorizados, lo que indica que el riesgo principal es la infiltración silenciosa antes que un ataque destructivo evidente.
- **Capacidad de Persistencia:** Los perfiles analizados muestran un tiempo de vida de sus operaciones que puede extenderse por meses, utilizando infraestructuras que rotan constantemente para evitar ser detectados por controles estándar.

Objetivos y Sectores Target



- **Gestión de Recursos Naturales:** Interés en documentos sobre licencias mineras, gestión de cuencas hidrográficas y políticas de protección forestal.
- **Soberanía y Ordenamiento Territorial:** Acceso a cartografía privilegiada, datos de fronteras y planes de desarrollo rural estratégicos.
- **Infraestructura Crítica Ambiental:** Monitoreo de sistemas de alerta temprana (clima, sismos) y redes de datos meteorológicos que son vitales para la prevención de desastres.
- **Cuentas de Alto Nivel:** El objetivo principal son los funcionarios con capacidad de decisión y administradores de sistemas que poseen privilegios extendidos sobre la red nacional.

Campañas Activas



- **Operaciones de Influencia y Desinformación:** Uso de identidades suplantadas para difundir información falsa o recolectar datos a través de engaños dirigidos a personal del sector ambiental.

- **Infiltración en Servicios de Datos:** Acciones orientadas a comprometer repositorios donde se centraliza la información de múltiples entidades ambientales, buscando un efecto de "compromiso en cascada".

- **Despliegue de Código para Exfiltración Silenciosa:** Campañas que utilizan documentos relacionados con normativas ambientales para introducir

software que extrae información de manera gradual hacia servidores externos.

- **Compromiso de Aplicaciones de Gestión:** Aprovechamiento de debilidades en portales institucionales para obtener acceso directo a las bases de datos de trámites y servicios ciudadanos.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

Para el desarrollo de esta sección, se ha realizado un mapeo estratégico entre las capacidades observadas en los adversarios analizados y el marco de referencia **MITRE ATT&CK**. Este análisis se enfoca en cómo estas tácticas impactarían específicamente al sector **Ambiente y Desarrollo Sostenible** (incluyendo su intersección con la agroindustria y la gestión de recursos naturales) en Colombia.

El siguiente mapeo identifica las fases del ciclo de ataque que representan el mayor riesgo para la integridad de los datos ambientales y la continuidad operativa de las instituciones. Se han seleccionado las técnicas más representativas de los actores identificados, justificando su relevancia para la protección de activos como la cartografía estratégica, datos meteorológicos y registros de propiedad rural.

ID	Tactica	Técnica	Justificación para el Sector Ambiente / Agro
T1566	Acceso Inicial	Phishing	Uso de correos con supuestas normativas ambientales o decretos para comprometer estaciones de trabajo institucionales.
T1078	Acceso Inicial	Valid Accounts	Uso de credenciales robadas de funcionarios para acceder a portales de trámites de licencias y servicios de tierras.
T1190	Acceso Inicial	Exploit Public-Facing Application	Aprovechamiento de vulnerabilidades en aplicaciones web del sector, como se evidencia en los reportes de incidentes graves de 2026.
T1059	Ejecución	Command and Scripting Interpreters	Ejecución de scripts automatizados para la recolección de metadatos de archivos sensibles dentro de los servidores.
T1543	Persistencia	Create or Modify System Process	Creación de servicios ocultos para asegurar que el acceso no se pierda tras reinicios de los sistemas de monitoreo.
T1071	Mando y Control	Application Layer Protocol	Comunicación con servidores externos simulando tráfico web legítimo (HTTP/S) para evadir herramientas de monitoreo.
T1005	Recolección	Data from Local System	Búsqueda y captura de documentos técnicos, mapas y bases de datos de recursos hídricos almacenados localmente.
T1021	Movimiento Lateral	Remote Services	Salto entre redes de diferentes dependencias territoriales utilizando conexiones de escritorio remoto mal configuradas.
T1041	Exfiltración	Exfiltration Over C2 Channel	Envío de información estratégica hacia el exterior utilizando los mismos canales de control establecidos por el adversario.
T1489	Impacto	Service Stop	Interrupción deliberada de sistemas de alerta temprana o monitoreo climático para generar desestabilización operativa.

Cadenas de Ataque Observadas

La cadena de ataque (Kill Chain) identifica las etapas secuenciales que los adversarios ejecutan para lograr sus objetivos dentro del sector Ambiente. En las operaciones analizadas para 2026, se observa una transición desde la intrusión técnica directa hacia ciclos de compromiso basados en la identidad y la confianza institucional. Estas cadenas no son lineales y a menudo implican múltiples reintentos en la fase de acceso inicial hasta lograr un punto de apoyo persistente.

Cadenas de ataque:

- Cadena basada en Documentación Técnica: El atacante envía un correo electrónico que simula ser una comunicación oficial sobre normativas de protección ambiental o gestión de tierras. El archivo adjunto contiene un código oculto que, al abrirse, utiliza funciones legítimas del sistema operativo para descargar un segundo componente más robusto desde un servidor externo.

- Cadena de Compromiso de Aplicaciones Web: Se identifican vulnerabilidades en los portales de servicios ciudadanos del sector. El adversario inserta scripts maliciosos en los formularios de contacto o carga

de documentos, permitiéndole capturar sesiones de administradores y escalar privilegios hacia el núcleo de la base de datos.

- Cadena de Infiltración vía Infraestructura Híbrida: Aprovechando la interconexión entre redes locales y servicios en la nube, los actores comprometen cuentas de correo con seguridad débil. Desde allí, se mueven lateralmente hacia los repositorios de almacenamiento compartido, donde plantan archivos dañinos que son descargados por otros funcionarios bajo una falsa apariencia de legitimidad.

Herramientas y Malware Específico

Para evitar la detección, los adversarios han optado por el uso de capacidades modulares que se adaptan al entorno de la víctima:

- **Software de Exfiltración de Documentos:** Código diseñado específicamente para rastrear extensiones de archivos comunes en el sector (mapas, hojas de cálculo, bases de datos) y enviarlos de manera fragmentada hacia el exterior para no generar alertas por alto tráfico de red.

- **Artefactos de Acceso Remoto:** Pequeños programas que se instalan en la memoria del equipo y permiten al atacante ver la pantalla, capturar lo que se escribe y ejecutar comandos como si estuviera físicamente frente al computador.

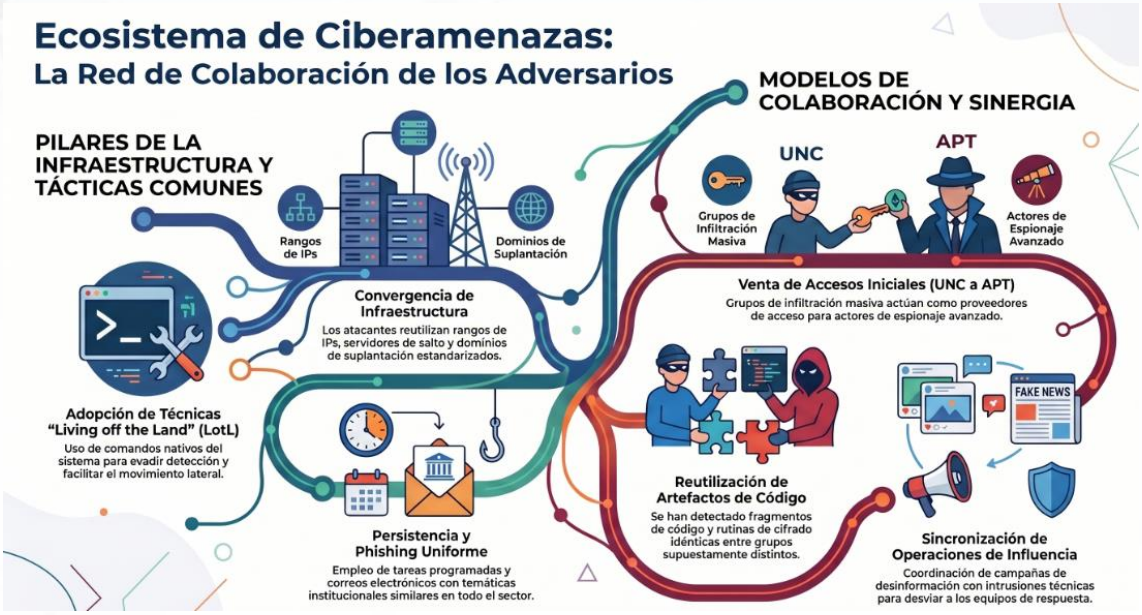
- **Scripts de Recolección de Credenciales:** Herramientas automatizadas que buscan contraseñas guardadas en navegadores web o en la configuración de aplicaciones de red, facilitando el movimiento hacia sistemas más sensibles.

- **Componentes de Ofuscación:** Capas de código que envuelven a las amenazas principales para que no puedan ser analizadas fácilmente por soluciones de seguridad estándar, cambiando su apariencia cada vez que son detectadas.

- **Software de Interrupción Operativa:** Códigos con capacidades destructivas o de bloqueo de servicios, utilizados principalmente para inhabilitar sistemas de monitoreo en tiempo real o borrar evidencia de una intrusión previa.

CORRELACIÓN ENTRE ACTORES Y GRUPOS

La sofisticación de las amenazas actuales sugiere que los adversarios no operan en silos aislados, sino que existe una interdependencia técnica que optimiza sus operaciones. La correlación entre los grupos identificados revela patrones de comportamiento donde la infraestructura y las metodologías de acceso son reutilizadas o compartidas. Esta convergencia dificulta la atribución precisa, pero permite establecer una defensa más robusta al identificar puntos comunes de falla. En el sector ambiental, esta correlación es crítica, ya que un acceso obtenido por un actor de recolección inicial puede ser posteriormente aprovechado por un actor de espionaje avanzado para fines estratégicos.



Infraestructura Compartida

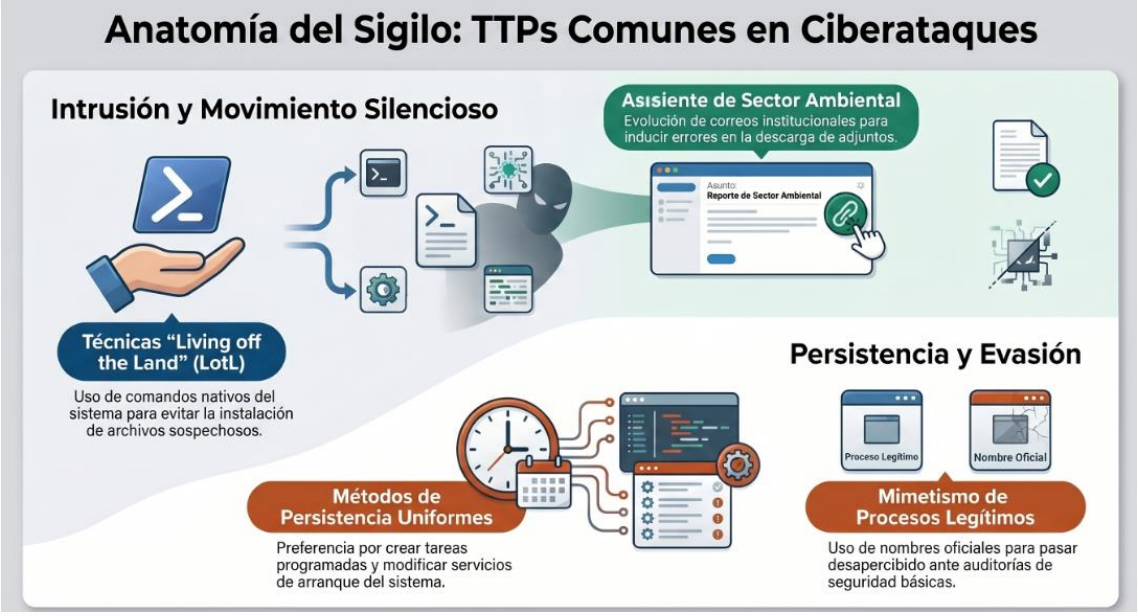
- **Uso de Servidores de Salto Comunes:** Se ha detectado que diferentes perfiles de adversarios utilizan los mismos rangos de direcciones IP para establecer sus nodos

de comando, lo que sugiere el uso de proveedores de servicios de red con políticas de seguridad laxas.

- **Dominios de Suplantación Estandarizados:** La estructura de los nombres de dominio utilizados para el robo de credenciales en entidades gubernamentales sigue patrones similares, empleando técnicas de variación tipográfica que parecen provenir de un mismo taller de desarrollo de señuelos.

- **Redes de Distribución de Contenido Dañino:** Se observa el uso recurrente de servicios de almacenamiento legítimos en la nube para alojar componentes maliciosos, permitiendo que múltiples grupos evadan bloqueos perimetrales al ocultarse tras tráfico de confianza.

Herramientas y TTPs Comunes



- **Adopción de Técnicas de "Vivir de la Tierra" (LotL):** La mayoría de los grupos analizados coinciden en el uso de comandos nativos del sistema operativo para evitar la instalación de archivos sospechosos, facilitando el movimiento lateral de manera silenciosa.

- **Métodos de Persistencia Uniformes:** Se identifica una preferencia compartida por la creación de tareas programadas y la modificación de servicios de arranque,

utilizando nombres que imitan procesos legítimos del sistema para pasar desapercibidos ante auditorías básicas.

- **Estructuras de Phishing Relacionadas:** Los formatos de los correos electrónicos dirigidos al personal del sector ambiental muestran una evolución paralela, utilizando temáticas institucionales similares para inducir al error en la descarga de archivos adjuntos.

Posibles Colaboraciones o Vínculos

- **Venta de Accesos Iniciales:** Es probable que grupos especializados en la infiltración masiva y el compromiso de cuentas (perfiles UNC) actúen como proveedores para actores de mayor nivel (perfiles APT), entregando accesos ya establecidos en redes del sector ambiental.

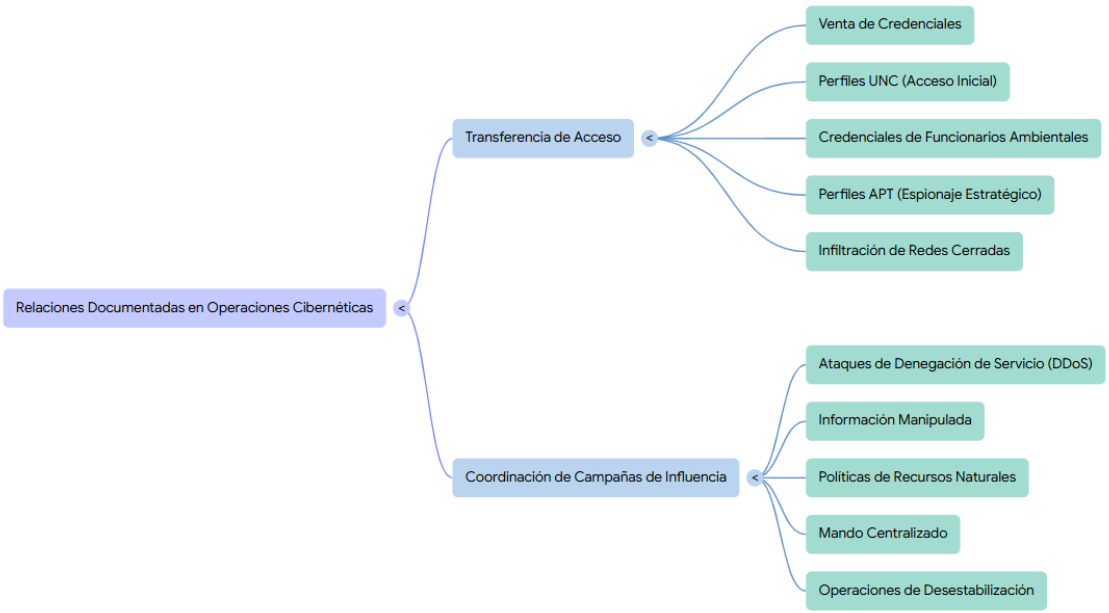
- **Sincronización de Operaciones de Influencia:** Se observa una alineación en los tiempos de ejecución de campañas de desinformación con actividades de intrusión técnica, lo que sugiere un nivel de coordinación estratégica para desviar la atención de los equipos de respuesta.

- **Reutilización de Artefactos de Código:** El análisis de los componentes dañinos revela fragmentos de código y rutinas de cifrado idénticas entre diferentes grupos, lo que indica el intercambio de recursos técnicos o la existencia de un ecosistema compartido de desarrollo de software para intrusión.

Visualización de Relaciones

La interconexión entre los adversarios analizados revela un ecosistema de amenazas maduro, donde las fronteras entre grupos de espionaje avanzado y operadores de acceso inicial son cada vez más difusas. La visualización de estas relaciones permite comprender que el sector Ambiente no enfrenta ataques aislados, sino un esfuerzo coordinado —directa o indirectamente— para comprometer la soberanía de los datos nacionales. A través del análisis de coincidencias en tiempos de actividad, registros de red y métodos de ejecución, se ha logrado trazar un mapa de dependencias que facilita la identificación de puntos críticos de control para la defensa proactiva.

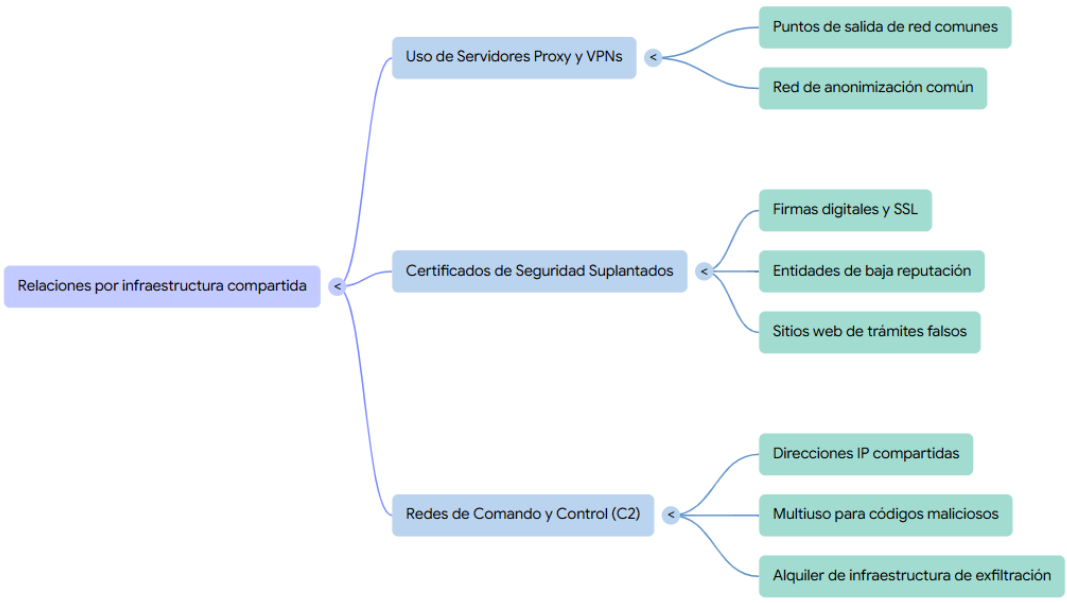
Relaciones directas documentadas:



- **Transferencia de Acceso (Venta de Credenciales):** Se ha documentado un vínculo operativo donde grupos de acceso inicial (perfiles UNC) obtienen credenciales de funcionarios ambientales que luego son utilizadas por actores de espionaje estratégico (perfiles APT) para infiltrar redes cerradas.

- **Coordinación de Campañas de Influencia:** Existe una relación directa en la cronología de ataques de denegación de servicio con la difusión de información manipulada sobre políticas de recursos naturales, sugiriendo un mando centralizado para operaciones de desestabilización.

Relaciones por infraestructura compartida

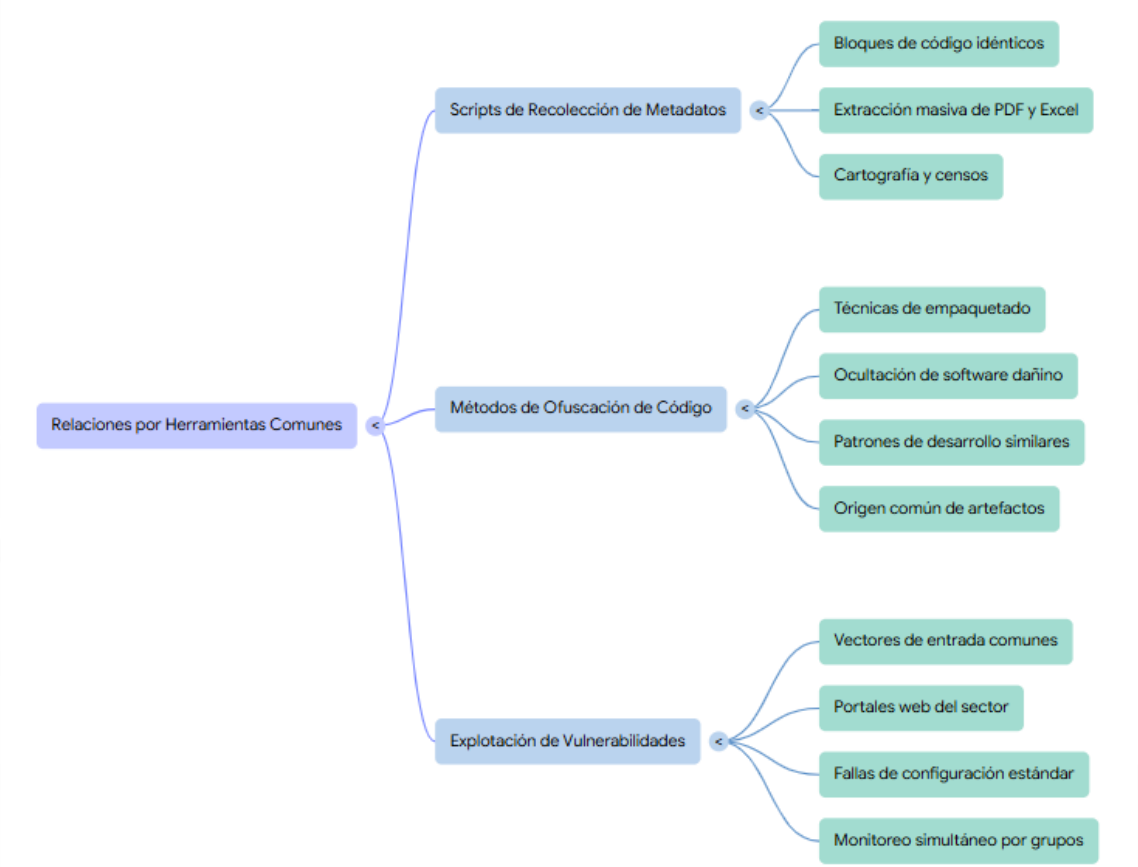


- **Uso de Servidores Proxy y VPNs:** Varios de los seis adversarios analizados han sido detectados utilizando los mismos puntos de salida de red para enmascarar su ubicación real, lo que indica el uso de una "red de anonimización" común.

- **Certificados de Seguridad Suplantados:** Se identifica el uso de firmas digitales y certificados SSL emitidos por las mismas entidades de baja reputación para validar sitios web falsos de trámites ambientales.

- **Redes de Comando y Control (C2) Multiuso:** Se han observado direcciones IP que actúan como receptores de datos para diferentes tipos de códigos maliciosos, sugiriendo que diversos actores alquilan la misma infraestructura de exfiltración.

Relaciones por herramientas comunes

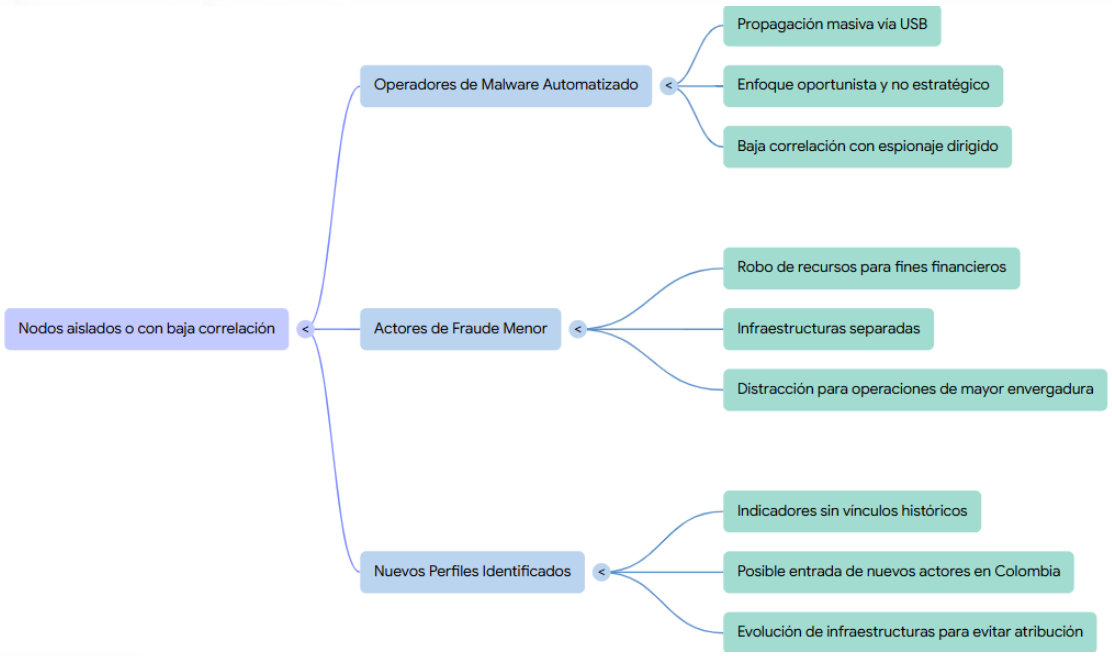


- **Scripts de Recolección de Metadatos:** Se ha identificado el uso de pequeños bloques de código idénticos entre diferentes grupos para la extracción masiva de información de archivos PDF y Excel relacionados con cartografía y censos.

- **Métodos de Ofuscación de Código:** El uso de técnicas de empaquetado para ocultar el software dañino muestra patrones de desarrollo similares, lo que apunta a un origen común en la creación de los artefactos de intrusión.

- **Explotación de Vulnerabilidades de Aplicación:** Los actores convergen en el uso de los mismos vectores de entrada contra portales web del sector, aprovechando fallas de configuración estándar que son monitoreadas por múltiples grupos simultáneamente.

Nodos aislados o con baja correlación (por ahora):



- **Operadores de Malware Automatizado:** Ciertos actores enfocados en la propagación masiva a través de dispositivos USB muestran una baja correlación con los grupos de espionaje dirigido, operando de manera más oportunista y menos estratégica.

- **Actores de Fraude Menor:** Grupos dedicados exclusivamente al robo de recursos para fines financieros inmediatos presentan infraestructuras separadas, aunque sus acciones pueden servir como distracción para operaciones de mayor envergadura.

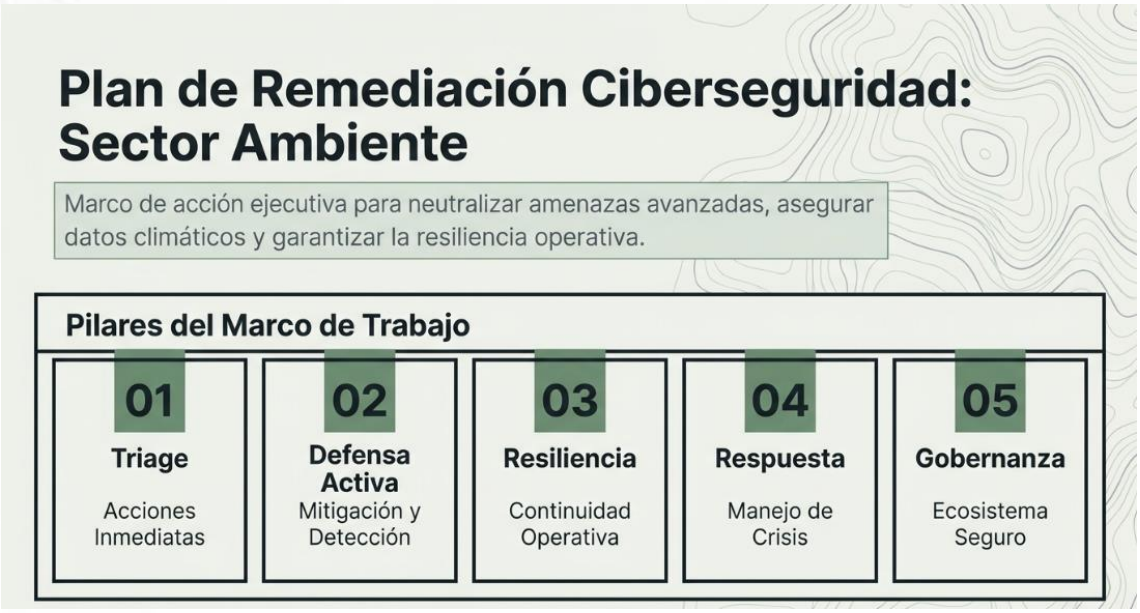
- **Nuevos Perfiles Identificados:** Algunos indicadores de compromiso recientes aún no presentan vínculos claros con los adversarios históricos, lo que sugiere la posible entrada de nuevos actores al escenario ambiental colombiano o la evolución de infraestructuras para evitar la atribución.

RECOMENDACIONES ESTRATÉGICAS

El fortalecimiento de la postura de ciberseguridad en el sector ambiental debe abordarse como una prioridad de seguridad nacional, dada la criticidad de la información gestionada (cartografía, recursos hídricos y biodiversidad). La estrategia propuesta se centra en la reducción drástica de la superficie de ataque, la segmentación lógica de redes institucionales y la protección rigurosa de la identidad digital. Se requiere un esfuerzo coordinado para que la seguridad no sea vista como un componente técnico aislado, sino como un habilitador de la soberanía ambiental frente a actores avanzados que buscan la exfiltración de inteligencia y la interrupción operativa.

Recomendaciones de Mitigación Técnica

Se deben implementar controles directos sobre la infraestructura para neutralizar los vectores de entrada explotados por grupos como los perfiles UNC analizados.



- **Endurecimiento de Aplicaciones Web:** Aplicar procesos de auditoría y cierre de vulnerabilidades en portales de trámites ambientales para prevenir el compromiso de aplicaciones, vector principal detectado en 2026.

- **Implementación de Autenticación Multifactor (MFA):** Desplegar MFA en todos los servicios de acceso remoto y correo institucional para mitigar el impacto del robo de credenciales.

- **Segmentación de Redes Críticas:** Aislar los sistemas de monitoreo climático y bases de datos geográficas del resto de la red administrativa para evitar movimientos laterales de los adversarios.

Recomendaciones de Detección y Monitoreo

Es imperativo aumentar la visibilidad sobre los eventos anómalos para detectar la presencia de actores de espionaje antes de que logren la exfiltración de datos.

- **Monitoreo de Comportamiento de Cuentas Privilegiadas:** Establecer alertas sobre patrones de inicio de sesión inusuales, especialmente en horarios no laborales o desde ubicaciones geográficas no esperadas.

- **Análisis de Tráfico Saliente:** Configurar sensores para identificar conexiones persistentes hacia servicios de almacenamiento en la nube no autorizados, utilizados comúnmente para la salida de información estratégica.

- **Cacería Proactiva de Amenazas (Threat Hunting):** Realizar búsquedas periódicas de indicadores de compromiso (IoCs) dentro de los registros de servidores para identificar persistencia silenciosa.

Recomendaciones de Resiliencia Operativa

El sector debe estar preparado para mantener sus funciones esenciales incluso ante un compromiso exitoso de su infraestructura digital.

Defensa Activa: Matriz de Control y Visibilidad

	Mitigación Preventiva	Monitoreo Detectivo
Vector 1: Robo de Credenciales	Implementación de Autenticación Multifactor (MFA) en todos los servicios de acceso remoto y correo institucional. →	Monitoreo de Cuentas Privilegiadas. Alertas sobre patrones de inicio de sesión inusuales (horarios no laborales o ubicaciones anómalas).
Vector 2: Compromiso de Aplicaciones	Endurecimiento de Apps Web. Auditoría y cierre de vulnerabilidades en portales de trámites ambientales. →	Cacería Proactiva de Amenazas (Threat Hunting). Búsquedas periódicas de IoCs en registros de servidores para identificar persistencia.
Vector 3: Movimiento Lateral	Segmentación de Redes Críticas. Aislamiento de sistemas de monitoreo climático y bases de datos geográficas de la red administrativa. →	Análisis de Tráfico Saliente. Sensores para identificar conexiones persistentes hacia almacenamiento en la nube no autorizado.

- **Esquemas de Respaldo Inmutables:** Asegurar que las copias de seguridad de los datos ambientales estén protegidas contra modificaciones y aisladas de la red principal para prevenir su cifrado o borrado.
- **Redundancia de Sistemas de Alerta Temprana:** Establecer canales de comunicación y procesamiento alternos para los sistemas de monitoreo climático y de desastres.
- **Pruebas de Continuidad del Negocio:** Realizar simulacros de recuperación ante desastres que incluyan escenarios de compromiso total de la identidad digital.

Recomendaciones de Gobernanza

La gestión del riesgo debe estar respaldada por políticas claras y un compromiso administrativo que garantice la sostenibilidad de las medidas de seguridad.

- **Actualización de Políticas de Acceso:** Revisar y aplicar el principio de "mínimo privilegio", asegurando que el personal solo tenga acceso a la información estrictamente necesaria para su rol.

- **Gestión de Riesgos de Terceros:** Establecer cláusulas de ciberseguridad rigurosas para contratistas y organismos internacionales que interactúan con los sistemas del sector ambiente.

- **Comités de Seguridad Sectorial:** Fomentar la colaboración técnica entre las diferentes entidades del sector (Ministerio, corporaciones regionales, institutos de investigación) para compartir inteligencia de amenazas.

Preparación ante Incidentes

La capacidad de respuesta rápida es el factor determinante para minimizar el impacto de las intrusiones de grupos avanzados.

- **Actualización de Planes de Respuesta:** Ajustar los protocolos de atención de incidentes para incluir procedimientos específicos contra actores de alta persistencia (APTs).
- **Entrenamiento de Equipos Técnicos:** Capacitar al personal de soporte en la preservación de evidencia digital y el aislamiento de sistemas infectados sin interrumpir la operación crítica.
- **Canales de Comunicación de Crisis:** Definir flujos de información claros hacia las autoridades nacionales de ciberseguridad ante eventos que comprometan la soberanía de los datos.

Acciones Inmediatas (Quick Wins)

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

- **Reinicio Forzado de Contraseñas Críticas:** Obligar al cambio de credenciales en cuentas de administración y sistemas expuestos a internet.
- **Bloqueo de Indicadores Identificados:** Integrar las direcciones IP y dominios maliciosos detectados en este análisis dentro de las listas de bloqueo de los firewalls institucionales.
- **Campaña de Alerta sobre Phishing:** Notificar al personal sobre la existencia de campañas de suplantación que utilizan temáticas de normatividad ambiental para distribuir malware.

CONCLUSIONES

1. **Elevación del Perfil de Riesgo Estratégico:** El sector ambiente ha dejado de ser un objetivo secundario para convertirse en un blanco de alto valor nacional. La presencia documentada de múltiples actores de espionaje avanzado indica que la información sobre recursos naturales, cartografía y biodiversidad es hoy un activo de seguridad nacional bajo asedio constante.

2. **Consolidación del Compromiso de Identidad como Vector Crítico:** El análisis revela que la mayoría de las intrusiones exitosas no explotan fallos técnicos complejos, sino la debilidad en la gestión de credenciales. El robo de identidades de funcionarios sigue siendo la "llave maestra" que permite a los adversarios operar de manera silenciosa y persistente dentro de la red estatal.

3. **Transición hacia Incidentes de Alta Severidad:** Los datos históricos muestran un cambio preocupante; los eventos han pasado de ser incidentes menores o fraudes simples a compromisos de aplicaciones y sistemas categorizados como **Graves**. Esto demuestra una mayor eficacia de los atacantes en sus fases de explotación y post-explotación.

4. **Vulnerabilidad en la Infraestructura Digital Territorial:** Existe una asimetría de seguridad entre el nivel nacional y el territorial. Mientras que Bogotá centraliza el volumen de ataques, regiones estratégicas para el medio ambiente muestran una exposición crítica, evidenciando que las entidades regionales requieren un fortalecimiento técnico inmediato para no ser el eslabón débil de la cadena.

5. **Correlación y Reutilización de Infraestructura:** La detección de infraestructuras compartidas y métodos de ataque uniformes sugiere que los adversarios operan dentro de un ecosistema colaborativo o de subcontratación de servicios de intrusión. Esto implica que una amenaza detectada en una entidad es, con alta probabilidad, un riesgo inminente para todo el sector ambiental.

6. **Imperativo de una Postura de Defensa Proactiva:** La resiliencia del sector no puede depender únicamente de herramientas de bloqueo tradicionales. Es fundamental adoptar estrategias de cacería de amenazas (Threat Hunting) y una arquitectura de confianza cero, asumiendo que el perímetro ya ha sido o será

vulnerado, para así minimizar el tiempo de detección y la capacidad de daño de los actores.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **Adversario:** Individuo o grupo de individuos con capacidades técnicas y motivaciones específicas (políticas, económicas o estratégicas) que realizan acciones dañinas contra la infraestructura digital del Estado.
- **Amenaza Persistente Avanzada (APT):** Operaciones de intrusión de alto nivel, generalmente respaldadas por recursos significativos, que buscan mantener un acceso prolongado y sigiloso a sistemas críticos.
- **Indicadores de Compromiso (IoCs):** Evidencias digitales (como direcciones IP, nombres de dominio o firmas de archivos) que señalan la presencia de una actividad maliciosa previa o en curso.
- **Tácticas, Técnicas y Procedimientos (TTPs):** El marco de comportamiento de un adversario. Las tácticas son los objetivos, las técnicas son los métodos para lograrlos y los procedimientos son las ejecuciones específicas observadas.
- **Ingeniería Social:** Tácticas de manipulación psicológica dirigidas a personas para que revelen información confidencial o realicen acciones que comprometan la seguridad.
- **Acceso Inicial:** La fase inicial de un ataque donde el adversario logra establecer un punto de entrada en la red o sistema de la víctima.

Infraestructura y Redes

- **Superficie de Ataque:** La suma total de todos los puntos de exposición (software, hardware, redes y personas) por los cuales un adversario puede intentar ingresar a un entorno digital
- **Mando y Control (C2):** Infraestructura externa utilizada por los atacantes para enviar instrucciones y recibir datos de los sistemas comprometidos dentro de la red institucional.

- **Movimiento Lateral:** Técnicas utilizadas por un atacante para navegar a través de la red interna después de haber comprometido un sistema inicial, buscando activos de mayor valor.

- **Exfiltración de Datos:** El proceso de transferencia no autorizada de información desde el interior de una organización hacia una ubicación externa controlada por el atacante.

- **Nodos de Salto:** Servidores o equipos intermedios utilizados por los adversarios para ocultar su ubicación real y dificultar la atribución de un ataque.

- **Arquitectura de Confianza Cero (Zero Trust):** Modelo de seguridad que asume que ninguna entidad es confiable por defecto, requiriendo verificación constante para cada acceso a la red.

Herramientas y Malware

- **Código Dañino (Malware):** Software diseñado específicamente para interrumpir, dañar o ganar acceso no autorizado a un sistema informático.

- **Scripts de Automatización:** Bloques de código ligero utilizados para ejecutar tareas repetitivas, como la recolección masiva de archivos o la búsqueda de vulnerabilidades en red.

- **Artefactos de Persistencia:** Modificaciones técnicas realizadas por el atacante en el sistema operativo para asegurar que su acceso se mantenga activo incluso después de un reinicio.

- **Phishing:** Método de entrega de amenazas que utiliza comunicaciones fraudulentas (correos, mensajes) para engañar al usuario y lograr la ejecución de malware o el robo de credenciales.

- **Ofuscación:** Técnicas utilizadas para ocultar el propósito real de un código malicioso, haciéndolo difícil de detectar por soluciones de seguridad tradicionales.

- **Software de Exfiltración:** Herramientas modulares configuradas para identificar y extraer tipos de archivos específicos (como bases de datos o mapas) sin generar alertas de red.

Sector

- **Soberanía Ambiental Digital:** La capacidad del Estado para proteger la integridad, disponibilidad y confidencialidad de la información estratégica relacionada con sus recursos naturales y territorio.

- **Infraestructura Crítica Ambiental:** Sistemas digitales esenciales para la supervivencia y el bienestar de la nación, como redes de monitoreo climático, sistemas de alertas tempranas y censos de recursos hídricos.

- **Activos Estratégicos:** Información de alto valor para la seguridad nacional, incluyendo cartografía, datos de biodiversidad y registros de propiedad rural.

- **Entidades Territoriales:** Organismos regionales encargados de la gestión ambiental local (como las Corporaciones Autónomas Regionales) que forman parte de la red de protección del sector.

- **Gobernanza de Ciberseguridad:** El marco de políticas, roles y responsabilidades que guían la toma de decisiones para proteger el ecosistema digital de una institución o sector.

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