TIC

Informe de apreciación

Sector Agro

COLCERT

Contenido

RESUMEN EJECUTIVO

En el sector agroindustrial en Colombia, la transformación digital y la integración de sistemas de control operativo (OT) —como la automatización de riego, sensores de agricultura de precisión y gestión de silos— 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 de la producción alimentaria, la integridad de los procesos de biotecnología y la estabilidad de la cadena de suministro nacional y de exportación.

Este informe utiliza inteligencia de amenazas de vanguardia para realizar un seguimiento riguroso al comportamiento de los actores que afectan el sector agro, 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 la infraestructura productiva nacional, permitiendo una toma de decisiones informada frente al riesgo digital que podría impactar la seguridad alimentaria y la economía del país.

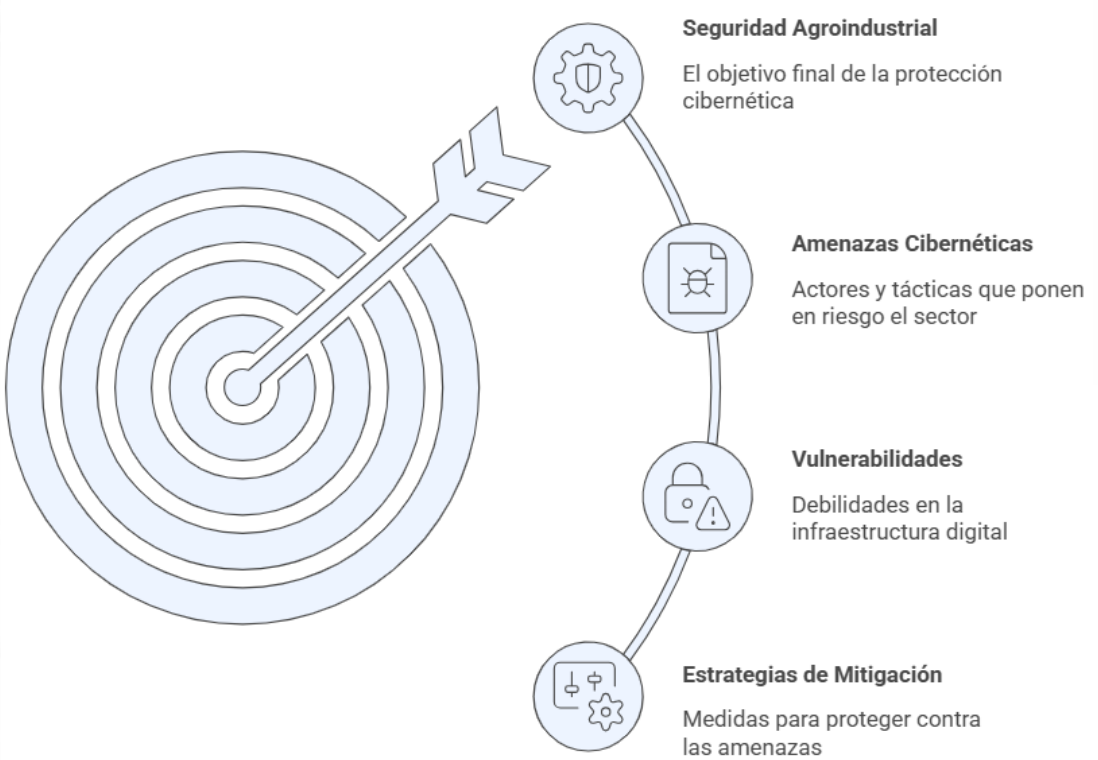
Lineamientos

- Seguimiento a actores que afectan el sector agroindustrial y de desarrollo rural en Colombia.
- Uso de inteligencia de amenazas para la identificación proactiva de vectores de ataque en entornos IT/OT.
- Priorización de fuentes de ciberinteligencia aplicables al contexto y geografía del país.
- Enfoque en infraestructuras productivas nacionales y sistemas de control industrial (ICS) aplicados al campo.
- Reducción de tiempos de detección y respuesta ante incidentes de alto impacto en la cadena de suministro.
- Fortalecimiento de la resiliencia cibernética de las entidades y gremios del sector agropecuario colombiano.

Informe de apreciación Sector Agro

COLCERT IN-20260708-040

TLP: CLEAR



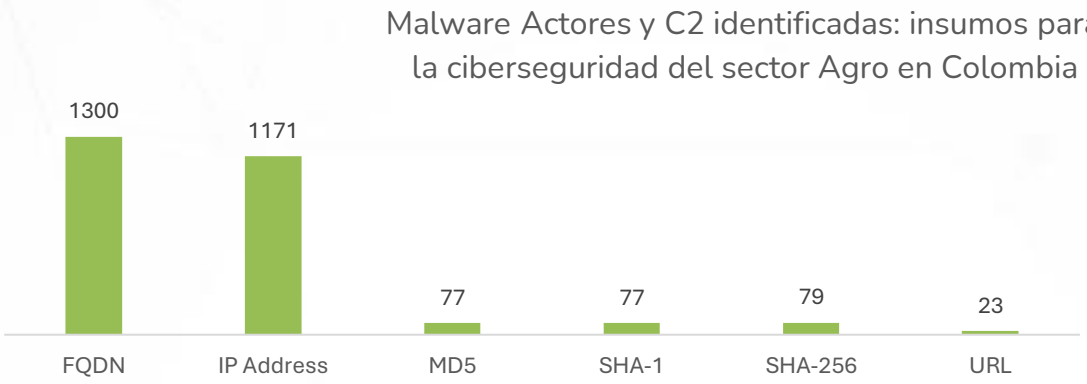
INTRODUCCIÓN

El presente informe analiza el panorama de amenazas cibernéticas que enfrentan las organizaciones del sector agroindustrial en Colombia. Ante un entorno de creciente digitalización en la cadena de suministro y la tecnificación del campo, se identifica una actividad persistente de grupos de ciberespionaje y crimen organizado. La convergencia entre sistemas de tecnología de la información (IT) y tecnologías de operación (OT) en el agro aumenta la superficie de ataque, exponiendo activos críticos a grupos con alta capacidad técnica y objetivos de interrupción operativa o robo de propiedad intelectual.

Puntos Clave:

- Presencia de actores de amenazas persistentes avanzadas (APT).
- Vulnerabilidad en la infraestructura crítica agropecuaria.
- Riesgo de espionaje industrial y robo de datos estratégicos.
- Amenaza de malware distribuido mediante técnicas de ingeniería social.
- Dependencia de la resiliencia operativa frente a ataques de interrupción.

Hallazgos Clave



- **Actividad de Grupos de Alta Sofisticación:** Se ha detectado la presencia de actores como **APT44** y **APT19**, conocidos por sus capacidades de espionaje a nivel global. En el contexto agro, estos grupos buscan recolectar inteligencia sobre tratados comerciales, biotecnología y procesos de producción.

- **Vector de Propagación Masiva:** Grupos como **UNC3840** utilizan métodos de distribución de malware altamente eficaces que pueden comprometer redes corporativas completas, facilitando el despliegue de cargas útiles más destructivas.

- **Ataques Orientados a Infraestructura:** La identificación de actores vinculados a ataques históricos contra redes eléctricas y sistemas industriales sugiere un riesgo latente para las plantas de procesamiento y sistemas de riego automatizados en Colombia.

- **Exfiltración de Información Estratégica:** El perfil de los adversarios indica un interés particular en el acceso a comunicaciones internas y bases de datos gubernamentales o privadas que regulan el sector agro, afectando la competitividad nacional.

Recomendaciones Prioritarias

- **Segmentación de Redes Críticas:** Aislar los entornos de producción agrícola y maquinaria industrial de las redes administrativas para prevenir el movimiento lateral de atacantes.
- **Programas de Concientización en Ingeniería Social:** Implementar capacitación continua para el personal del sector, dado que muchos de los actores identificados utilizan el engaño como puerta de entrada.
- **Monitoreo Activo de Activos Digitales:** Establecer una vigilancia constante sobre las comunicaciones y el tráfico de red para identificar patrones de comportamiento asociados a los grupos detectados.
- **Actualización y Fortalecimiento de Sistemas:** Priorizar el cierre de brechas de seguridad en software de gestión agrícola y sistemas de control que suelen quedar fuera de los ciclos de actualización tradicionales.

Conclusión Estratégica

La seguridad del sector agroindustrial es un pilar fundamental para la estabilidad económica y alimentaria de Colombia. La presencia de adversarios con capacidades de nivel estatal subraya que el agro ya no es un objetivo secundario, sino un frente activo

en el ciberespacio. La estrategia debe evolucionar de un enfoque puramente reactivo hacia una postura de resiliencia proactiva, donde la protección de la propiedad intelectual y la continuidad de las operaciones en campo sean prioridades de alta gerencia.

OBJETIVO Y ALCANCE

Objetivo

El objetivo de este documento es informar a las partes interesadas del sector agro sobre el panorama de riesgos derivado de la actividad de grupos de amenazas detectados en territorio colombiano, facilitando la toma de decisiones para proteger la infraestructura crítica nacional.

Alcance

Este informe comprende el análisis de las tácticas y perfiles de los grupos de adversarios con actividad reciente en Colombia, evaluando su impacto potencial específicamente en la cadena de valor agrícola, desde la producción primaria hasta la exportación.

Este informe abarca:

- Perfiles de adversarios APT detectados.
- Análisis de riesgo por espionaje y sabotaje.
- Evaluación de vulnerabilidades sectoriales.
- Estrategias de mitigación de amenazas.

Informe de apreciación Sector Agro

COLCERT IN-20260708-040

TLP: CLEAR

CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR

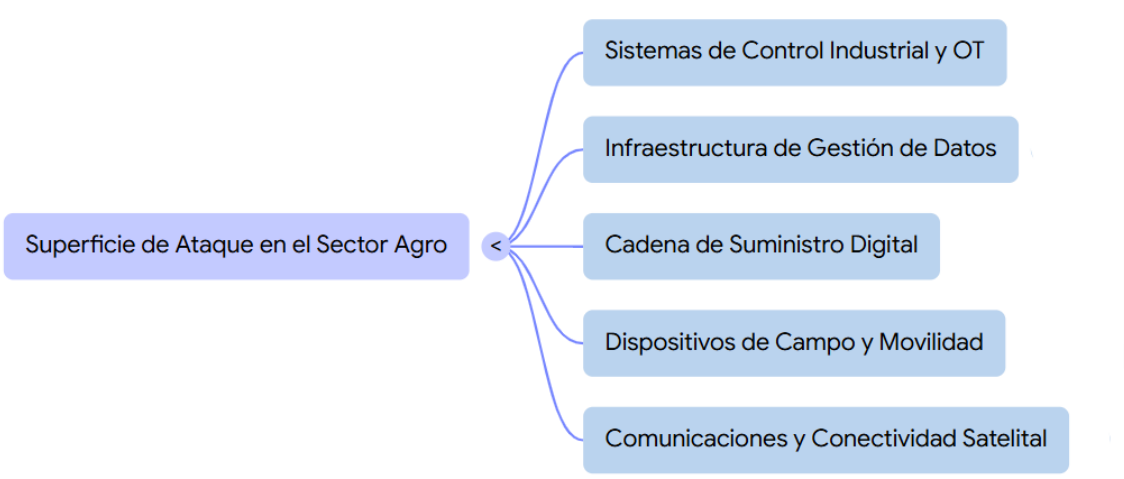
Definición y Entendimiento del Sector

El sector agroindustrial en Colombia es un motor económico fundamental que integra la producción primaria (agrícola, pecuaria y forestal) con procesos de transformación industrial y redes de distribución global. Este sector ha experimentado una transformación digital acelerada, adoptando tecnologías de precisión, Internet de las Cosas (IoT) para el monitoreo de cultivos y plataformas digitales para la gestión de la cadena de suministro. Sin embargo, esta modernización lo sitúa en el centro de intereses geopolíticos y económicos, convirtiéndolo en un objetivo para actores que buscan desestabilizar la seguridad alimentaria o extraer ventajas competitivas mediante el acceso no autorizado a datos de innovación y comercio.

Superficie de Ataque

La superficie de ataque en el sector agro se ha expandido significativamente, dejando de ser un entorno aislado para convertirse en un ecosistema hiperconectado. La convergencia entre la tecnología de oficina y los sistemas de control en campo crea

múltiples puntos de entrada que los adversarios pueden explotar para infiltrarse en las organizaciones.



- **Sistemas de Control Industrial y OT:** Incluye la maquinaria automatizada, sensores de humedad, sistemas de riego y estaciones climáticas que, al estar conectados, pueden ser manipulados para detener la producción física.
- **Infraestructura de Gestión de Datos:** Bases de datos que contienen información crítica sobre patentes de semillas, fórmulas de fertilizantes, registros sanitarios y estrategias de precios de exportación.
- **Cadena de Suministro Digital:** Portales de proveedores y plataformas de logística que, de ser comprometidos, permiten a los atacantes realizar movimientos laterales hacia las redes principales de las empresas agroindustriales.
- **Dispositivos de Campo y Movilidad:** El uso de dispositivos móviles y tabletas por parte de técnicos y operarios en zonas rurales, que a menudo carecen de perímetros de seguridad robustos, facilitando el acceso inicial a los adversarios.
- **Comunicaciones y Conectividad Satelital:** Canales utilizados para la transmisión de datos desde zonas remotas, los cuales pueden ser interceptados o interferidos por grupos con capacidades avanzadas como los identificados en este análisis.

Informe de apreciación Sector Agro

COLCERT IN-20260708-040

TLP: CLEAR

PANORAMA ACTUAL DE AMENAZAS

El panorama de ciberamenazas en Colombia para el año 2026 revela una convergencia crítica entre el espionaje dirigido y el cibercrimen oportunista, afectando directamente la estabilidad del sector agroindustrial. Se observa un incremento significativo en el uso de inteligencia artificial para la automatización de ataques, reduciendo drásticamente los tiempos entre el descubrimiento de vulnerabilidades y su explotación activa. Grupos con motivaciones financieras y políticas han intensificado sus operaciones de ransomware bajo modalidades de triple extorsión, donde la interrupción de la cadena de suministro agroalimentaria se utiliza como palanca de presión reputacional y económica. Adicionalmente, el aumento en el robo de identidades mediante técnicas de phishing avanzado ha facilitado el acceso inicial a infraestructuras críticas, permitiendo a los adversarios persistir en las redes de producción y exfiltrar datos estratégicos sin ser detectados de manera inmediata.

TITULO	FECHA	FUENTE / ENLACE
Incidentes de ciberseguridad reportados por el Ministerio de Agricultura y Desarrollo Rural (2020–2026)	2026-04-06 (último incidente visible)	Datos.gov
Ciberseguridad en el sector agropecuario: vulnerabilidades en sistemas de información y IoC agrícola (Sumapaz, Colombia)	2024 (publicado)	Epsir.net
IoT y ciberseguridad en el sector agroalimentario: ¿aliados o riesgo?	2025-11-19	Esedls.com
La importancia de la ciberseguridad en agricultura: riesgos y buenas prácticas	2026-02-26	agrotechcampus
Ciberseguridad en sistemas de información agropecuarios: desafíos estratégicos para el sector agroindustrial	2024	Magazineasce.com

Tipología de Eventos Identificados

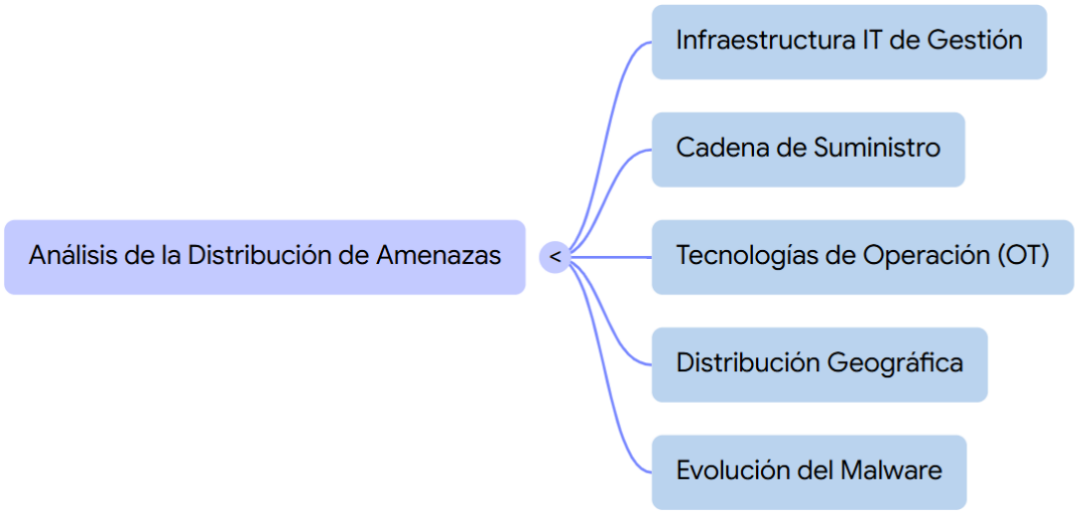
La identificación de eventos de seguridad en el sector agro colombiano permite categorizar las tácticas de los atacantes según la naturaleza del rastro digital que dejan. Durante el periodo analizado, se observa una predominancia de eventos relacionados con el acceso inicial y la persistencia silenciosa. Estos eventos no actúan de forma aislada; suelen formar parte de una cadena de ataque diseñada para comprometer la

integridad de la producción y la confidencialidad de las fórmulas y procesos de transformación industrial.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector
Hashes de Malware	Alto (+500 variantes)	Repositorios de amenazas, análisis de archivos, telemetría de endpoints.	Identificación de herramientas de espionaje diseñadas para el robo de propiedad intelectual biotecnológica.
Dominios y URLs	Moderado (150 activos)	Análisis de tráfico de red, registros DNS, reportes de incidentes.	Bloqueo de sitios de suplantación (phishing) dirigidos a proveedores de la cadena de suministro agrícola.
Direcciones IP (C2)	Constante (Cambio dinámico)	Honeypots, registros de firewalls industriales, inteligencia de amenazas.	Prevención de conexiones salientes desde sensores de campo o maquinaria hacia servidores externos.
Patrones de Comportamiento	Bajo (Complejos)	Análisis forense (DFIR), frameworks de tácticas y técnicas.	Detección de persistencia en redes que gestionan la logística y distribución de productos hacia puertos.
Certificados Digitales	Muy Bajo (Específicos)	Bases de datos de autoridades de certificación, análisis de binarios.	Mitigación del riesgo de software malicioso "firmado" en estaciones de control de riego o silos.

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

Análisis de la Distribución de Amenazas



- Concentración en Infraestructura IT de Gestión: La mayor densidad de eventos de amenaza se concentra en los sistemas de planificación de

recursos (ERP) y correos corporativos, donde actores como APT19 buscan información sobre acuerdos comerciales y exportaciones.

- Ataques Dirigidos a la Cadena de Suministro: Se identifica una distribución creciente de amenazas que afectan a terceros y proveedores de servicios tecnológicos para el agro, utilizando a estos colaboradores como puente para alcanzar las redes de las grandes agroindustrias.

- Persistencia en Tecnologías de Operación (OT): Aunque el volumen es menor, la gravedad de las amenazas detectadas en sistemas de control de procesos (sensores, automatización de silos) es crítica, con técnicas similares a las empleadas por APT44 en otros sectores de infraestructura.

- Distribución Geográfica de Sensores de Amenaza: Los indicadores muestran una mayor actividad en nodos regionales de procesamiento (como el Eje Cafetero, Valle del Cauca y la zona bananera), donde la conectividad digital es más robusta y la concentración de activos es mayor.

- Evolución del Malware según el Adversario: La distribución de las cargas útiles revela que grupos como UNC3840 prefieren malware de propagación rápida para generar volumen, mientras que los grupos tipo APT optan por herramientas personalizadas de bajo perfil para evitar la detección por firmas tradicionales.

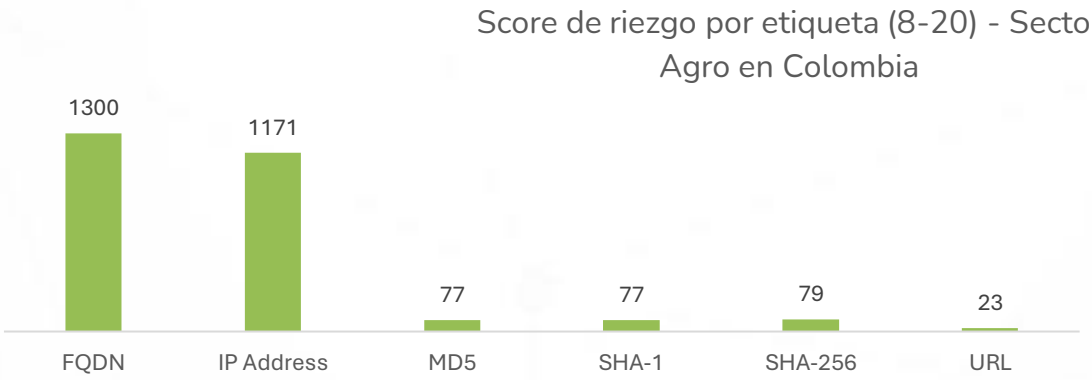
El análisis del registro histórico de incidentes para el sector de Agricultura y Desarrollo Rural revela un panorama de amenazas persistente con una evolución clara desde fallos de disponibilidad y suplantaciones básicas hacia compromisos de información y aplicaciones mucho más sofisticados. Se observa que, aunque el fraude mediante el uso no autorizado de recursos y phishing mantiene un volumen constante catalogado como "Menor", la aparición recurrente de "Sistemas Vulnerables" y "Compromiso de Aplicaciones" con calificación "Grave" indica una explotación dirigida de debilidades en la infraestructura técnica.

Fecha	Clasificación	Tipo de Incidente	Descripción	Importancia
6/04/2026	Nacional	Compromiso de Información	Acceso no Autorizado a Información	Grave
24/11/2025	Nacional	Vulnerable	Sistema Vulnerable	Grave
24/11/2025	Nacional	Vulnerable	Sistema Vulnerable	Grave
4/09/2025	Nacional	Contenido Dañino	Servidor C&C (Comando y Control)	Grave
31/07/2025	Nacional	Vulnerable	Sistema Vulnerable	Grave

Especialmente preocupante es la tendencia registrada entre 2023 y 2026, donde los incidentes de modificación no autorizada y acceso a información crítica han escalado a niveles de importancia "Muy Grave", sugiriendo que el sector es un objetivo prioritario para el robo de datos estratégicos y la interrupción operativa.

INDICADORES DE COMPROMISO (IoCs)

Los Indicadores de Compromiso (IoCs) constituyen la evidencia digital técnica que permite identificar actividades maliciosas dentro de la infraestructura del sector agropecuario. En un entorno donde la convergencia IT/OT es cada vez más estrecha, la detección temprana de estos artefactos es vital para prevenir el sabotaje de procesos biotecnológicos, la interrupción de cadenas de frío o el robo de propiedad intelectual sobre semillas y cultivos. El monitoreo de estos indicadores permite a los analistas de seguridad pasar de una postura reactiva a una defensa proactiva, bloqueando infraestructuras enemigas antes de que se consolide el compromiso total de la red.



Análisis Cuantitativo de Inteligencia

- **Prevalencia de Infraestructura de Red:** Se observa un volumen significativo de direcciones IP y nombres de dominio (FQDN) activos, con puntuaciones de riesgo que sugieren una infraestructura de comando y control (C2) distribuida, diseñada para evadir bloqueos geográficos.

- **Diversidad de Firmas de Archivo:** Existe una distribución variada de hashes (MD5, SHA-1, SHA-256) asociados a cargadores de malware, lo que indica que

los adversarios están rotando constantemente sus herramientas para evadir soluciones de seguridad basadas en firmas tradicionales.

- **Ciclo de Vida de los Indicadores:** La inteligencia recolectada muestra una alta tasa de "reciclaje" de infraestructura; IPs detectadas en campañas contra otros sectores estratégicos están siendo reorientadas hacia el sector agroindustrial colombiano.

- **Concentración de Amenazas en Capa de Aplicación:** Se identifica un enfoque persistente en la creación de dominios que suplantan herramientas legítimas de seguridad o gestión técnica, buscando engañar a los operadores de sistemas de control industrial.

Resumen de IoCs Relevantes

La siguiente tabla consolida los componentes técnicos críticos extraídos de las fuentes de inteligencia, proporcionando una base para la implementación de reglas de detección y bloqueo en perímetros de red y dispositivos finales.

Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
FQDN (Nombres de Dominio)	Dominios como core1draw.com o white-check-security.tools utilizados para el despliegue de malware o suplantación de servicios.	Crítico
Direcciones IP (C2)	Direcciones como 185.220.101.169 asociadas a nodos de salida y servidores de control de botnets activos.	Alto
Hashes de Archivo (MD5/SHA)	Firmas digitales de archivos maliciosos (ej. 5294aaf2ff805...) que deben ser buscadas en sistemas de archivos y memoria.	Crítico
Indicadores de Persistencia	Artefactos técnicos que permiten al malware permanecer activo tras reinicios del sistema en estaciones de trabajo administrativas.	Alto
Registros de Telemetría (Touched At)	Marcas de tiempo de actividad reciente que confirman la vigencia operativa de la infraestructura del atacante en mayo de 2026.	Medio

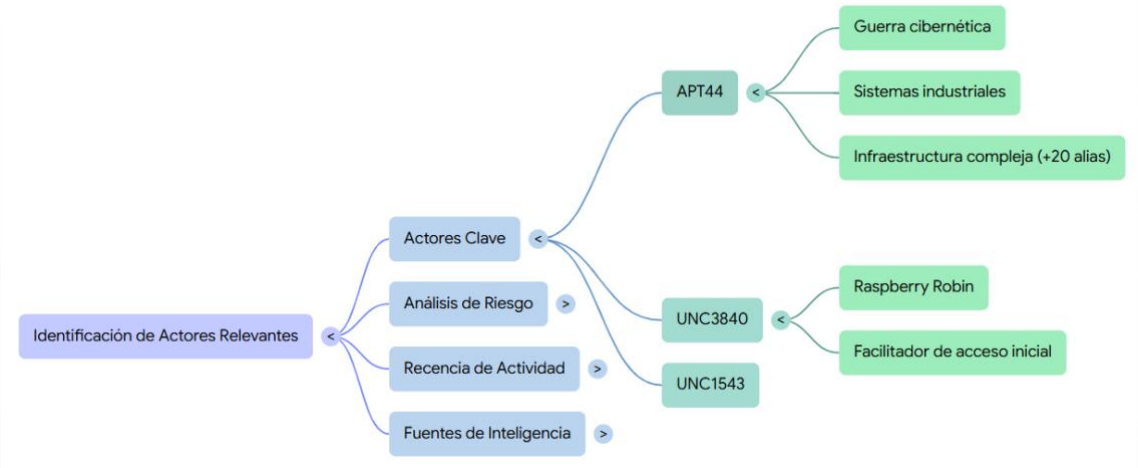
ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

El ecosistema de amenazas para el sector agroindustrial en Colombia está compuesto por una mezcla de grupos con motivaciones de espionaje nacional y actores orientados al beneficio económico. El análisis de los perfiles permite identificar una clara especialización en las fases de intrusión y exfiltración de datos sensibles.

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Amenaza Persistente Avanzada (APT)	2	**APT44** (Sandworm), **APT19** (Codoso)	Riesgo crítico de sabotaje a infraestructuras y robo de patentes biotecnológicas.
Grupos de Intrusión Dirigida (UNC)	2	**UNC1543**, **UNC3840**	Compromiso de la cadena de suministro y despliegue de malware para extorsión financiera.

Identificación de Actores Relevantes

La identificación de estos actores se basa en la correlación de sus tácticas, técnicas y procedimientos (TTPs) observados en campañas recientes dentro del territorio nacional. Se ha determinado que grupos como **APT44** poseen capacidades de guerra cibernética que podrían ser reorientadas hacia sistemas industriales del campo, mientras que grupos como **UNC3840** (asociado a Raspberry Robin) actúan como facilitadores de acceso inicial, permitiendo que otros actores más peligrosos penetren en las redes corporativas de las grandes agroindustrias colombianas.



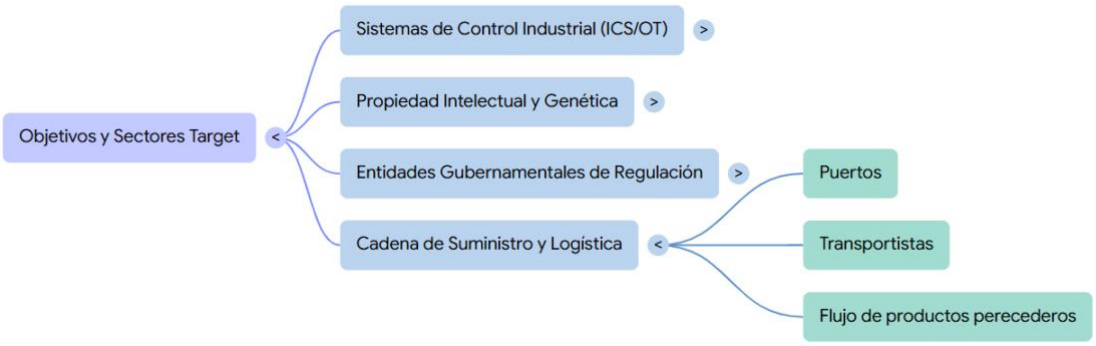
- **Prevalencia de Grupos APT:** El 50% de los actores identificados poseen capacidades de nivel estatal, lo que eleva el riesgo de ataques diseñados para permanecer ocultos por largos periodos (dwell time).

- **Volumen de Alias y Atribuciones:** El actor **APT44** presenta la mayor cantidad de fuentes y alias (más de 20), lo que refleja una infraestructura compleja y una alta capacidad de mutación operativa para evadir sanciones y bloqueos.

- **Recencia de Actividad:** Los registros de inteligencia muestran actividad persistente durante el primer cuatrimestre de 2026, con actualizaciones críticas en los perfiles de **UNC1543** y **UNC3840** en mayo del presente año.

- **Diversidad de Fuentes de Verificación:** La inteligencia proviene de una amalgama de fuentes de alta fidelidad, incluyendo Google Threat Intelligence, MISP y firmas líderes en ciberseguridad, lo que otorga una confianza alta a los perfiles presentados.

Objetivos y Sectores Target



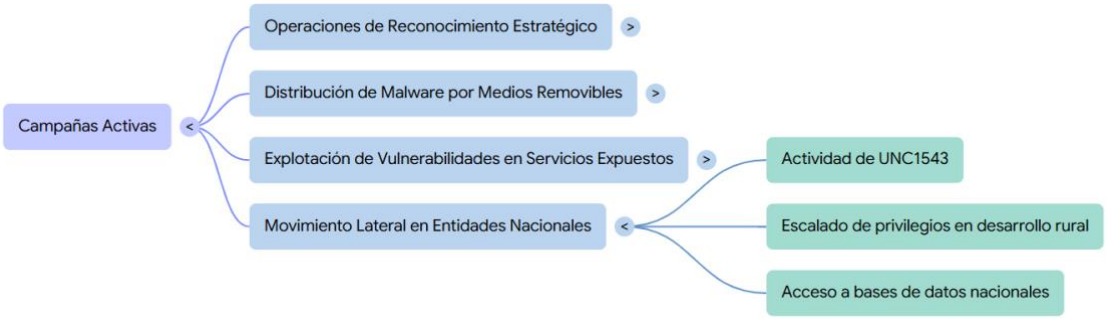
- **Sistemas de Control Industrial (ICS/OT):** Los actores buscan vulnerar los sistemas que gestionan el procesamiento de granos, control de clima en invernaderos y automatización de maquinaria pesada.

- **Propiedad Intelectual y Genética:** El robo de datos sobre mejoramiento de semillas, fórmulas de fertilizantes y procesos de exportación es un objetivo primario para grupos de espionaje.

- **Entidades Gubernamentales de Regulación:** El seguimiento a las instituciones que norman el desarrollo rural en Colombia para anticipar cambios en tratados comerciales o políticas de tierras.

- **Cadena de Suministro y Logística:** Compromiso de puertos y transportistas para interrumpir el flujo de productos perecederos hacia mercados internacionales.

Campañas Activas



- **Operaciones de Reconocimiento Estratégico:** Grupos vinculados a **APT19** mantienen campañas de recolección de información mediante el compromiso de cuentas de correo de directivos del sector.

- **Distribución de Malware mediante Medios Removibles:** Campañas activas de **UNC3840** que utilizan dispositivos USB y otros vectores físicos para saltar el "air-gap" en redes de control industrial aisladas.

- **Explotación de Vulnerabilidades en Servicios Expuestos:** Identificación de intentos de intrusión aprovechando debilidades en plataformas de gestión agrícola basadas en la nube que carecen de autenticación multifactor.

- **Campañas de Movimiento Lateral en Entidades Nacionales:** Actividad detectada de **UNC1543** orientada a escalar privilegios dentro de redes institucionales relacionadas con el desarrollo rural para obtener acceso a bases de datos nacionales.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

El uso del framework MITRE ATT&CK permite estandarizar la comprensión del comportamiento de los atacantes, facilitando la creación de estrategias de defensa basadas en inteligencia. Para el sector agroindustrial, este mapeo es crucial ya que permite identificar cómo los grupos APT y de cibercrimen logran transicionar desde el compromiso de una estación de trabajo administrativa hasta el control de sistemas críticos de producción o la exfiltración de secretos comerciales y biotecnológicos.

ID	Tactica	Técnica	Justificación para el Sector Agroindustrial
T1566	Acceso Inicial	Phishing	Uso de correos dirigidos a directivos con supuestos informes de precios de mercado para ganar acceso.
T1190	Acceso Inicial	Exploit Public-Facing Application	Explotación de vulnerabilidades en portales de gestión logística o de exportación expuestos a internet.
T1059	Ejecución	Command and Scripting Interpreter	Uso de scripts en Python o PowerShell para automatizar la recolección de datos en servidores de gestión de cultivos.
T1133	Persistencia	External Remote Services	Mantenimiento del acceso mediante el uso de VPNs o RDP mal configurados en plantas de procesamiento.
T1078	Persistencia	Valid Accounts	Uso de correos dirigidos a directivos con supuestos informes de precios de mercado para ganar acceso.
T1083	Descubrimiento	File and Directory Discovery	Búsqueda de archivos relacionados con fórmulas de agroquímicos, patentes de semillas y planes deexpansión.
T1046	Descubrimiento	Network Service Scanning	Escaneo de redes internas para identificar controladores lógicos programables (PLC) en sistemas de riego.
T1071	Mando y Control	Application Layer Protocol	Comunicación del malware con servidores externos usando tráfico HTTP/HTTPS para ocultarse tras el tráfico normal.
T1041	Exfiltración	Exfiltration Over C2 Channel	Envío de bases de datos de clientes y proveedores hacia servidores controlados por actores como APT19.
T1486	Impacto	Data Encrypted for Impact	Despliegue de ransomware para detener la cadena de frío o la distribución de productos perecederos.

Este mapeo demuestra que la defensa debe ser multicapa. Mientras que las tácticas de **Acceso Inicial** se mitigan con concienciación y robustecimiento de perímetros, las tácticas de **Descubrimiento** y **Mando y Control** requieren de un monitoreo interno avanzado y segmentación de red para evitar que un incidente en la oficina administrativa detenga la operación en el campo.

Cadenas de Ataque Observadas

El análisis de las intrusiones en el sector agroindustrial permite identificar patrones de comportamiento lógico que los adversarios repiten para alcanzar sus objetivos. Estas cadenas de ataque no son lineales, sino que se adaptan a las medidas de seguridad presentes en cada organización, buscando siempre el camino de menor resistencia, ya sea a través del eslabón humano o de vulnerabilidades técnicas en sistemas desatendidos.

Fases de la Cadena de Intrusión:

- Reconocimiento y Vigilancia.
- Preparación de Capacidades.
- Entrega de Cargas Útiles.
- Explotación de Vulnerabilidades.
- Instalación de Persistencia.
- Comando y Control (C2).
- Acciones sobre Objetivos (Exfiltración/Sabotaje).

Cadenas de ataque:

- **Intrusión mediante Ingeniería Social y Phishing:** Es el método predominante para el acceso inicial. Los atacantes envían correos electrónicos altamente personalizados dirigidos a personal administrativo o técnico, adjuntando documentos maliciosos que, al ser ejecutados, descargan troyanos de acceso remoto (RAT) para comprometer la estación de trabajo.

- **Explotación de Activos Expuestos:** Los adversarios escanean la infraestructura de red en busca de servicios de acceso remoto (VPN, RDP) o plataformas de gestión agrícola basadas en web que no cuentan con parches de seguridad actualizados, permitiendo la ejecución de código de forma remota.

- **Compromiso de la Cadena de Suministro Digital:** Se observa el uso de actualizaciones de software legítimo comprometidas o el acceso a través de las redes de proveedores de servicios tecnológicos (Managed Service Providers) que tienen conexiones directas a los sistemas del cliente final.

- **Movimiento Lateral desde IT hacia OT:** Una vez que el atacante tiene control sobre la red administrativa (IT), utiliza herramientas de administración legítimas para saltar hacia las redes de control industrial (OT), buscando alcanzar los controladores lógicos (PLC) que operan maquinaria de campo o plantas de procesamiento.

- **Exfiltración Silenciosa de Datos:** En ataques de espionaje industrial, los actores establecen canales de comunicación cifrados para extraer de forma gradual planos técnicos, bases de datos de investigación genética o contratos comerciales, minimizando las alertas por volumen de tráfico.

Herramientas y Malware Específico

- Malware de Acceso Remoto (RAT): Herramientas diseñadas para otorgar control total al atacante sobre el sistema infectado, permitiéndole navegar por archivos, capturar pulsaciones de teclado y activar dispositivos periféricos sin que el usuario lo note.

- Scripts de Automatización y Reconocimiento: Uso de lenguajes de programación como Python y PowerShell para realizar inventarios rápidos de la red, identificar activos críticos y automatizar la búsqueda de información sensible bajo patrones específicos.

- Herramientas de "Living off the Land" (LotL): Uso de aplicaciones legítimas del sistema operativo (como administradores de tareas o utilidades de red) para realizar actividades maliciosas, lo que dificulta la distinción entre el trabajo normal del administrador y la actividad del atacante.

- Cargadores de Malware (Loaders): Programas ligeros cuya única función es establecer una conexión inicial segura para descargar y ejecutar malware más pesado y complejo una vez que han verificado que no están en un entorno de análisis (sandbox).

- Web Shells: Scripts cargados en servidores web comprometidos que permiten al atacante ejecutar comandos de forma remota a través de una interfaz de navegador, manteniendo el acceso incluso si se cambian las contraseñas de los usuarios.

CORRELACIÓN ENTRE ACTORES Y GRUPOS

El análisis de ciberinteligencia permite identificar puntos de convergencia entre los distintos adversarios que amenazan el sector agroindustrial en Colombia. A menudo, lo que parece ser una serie de ataques aislados revela una red interconectada donde diferentes grupos comparten recursos, infraestructura o metodologías. Esta correlación es fundamental para entender que la defensa contra un actor específico, como un grupo de ransomware, puede proporcionar inmunidad contra actores de espionaje más avanzados que utilizan vectores de entrada similares. La colaboración entre estos grupos, ya sea intencional o mediante la compra de accesos en mercados clandestinos, aumenta la peligrosidad y la resiliencia de las campañas dirigidas al campo colombiano.

Infraestructura Compartida

- Uso de Nodos de Salida y Proxies Comunes: Se ha detectado que actores como UNC3840 y ciertos subgrupos de APT44 utilizan la misma red de direcciones IP para sus operaciones de comando y control (C2), lo que sugiere el uso de servicios de anonimización compartidos o proveedores de hosting que ignoran actividades ilícitas.

- Registradores de Dominios y Certificados: Diversos adversarios registran sus dominios de ataque bajo los mismos proveedores, empleando patrones de nomenclatura similares que simulan servicios de seguridad o actualizaciones de software, facilitando la gestión de múltiples campañas bajo una misma arquitectura lógica.

- Reutilización de Servidores de Exfiltración: En varios incidentes reportados, la infraestructura utilizada para alojar datos robados de una entidad agropecuaria ha sido vinculada previamente a campañas de robo de información en otros sectores estratégicos, evidenciando una optimización de recursos por parte de los atacantes.

Herramientas y TTPs Comunes

- Estandarización en el Uso de RATs: Tanto APT19 como grupos de intrusión dirigida emplean variantes de troyanos de acceso remoto con funciones similares, como la capacidad de captura de pantalla y robo de credenciales, adaptándolos mínimamente para evadir detecciones específicas.

- Abuso de Herramientas de Administración Legítimas: Existe una convergencia en el uso de utilidades del sistema (como herramientas de red y scripts de gestión) para realizar movimientos laterales. Esta táctica de "vivir de la tierra" es compartida por casi todos los actores identificados para minimizar su rastro digital.

- Similitud en Vectores de Phishing: El diseño de los señuelos, centrados en documentos técnicos de agricultura o notificaciones gubernamentales de desarrollo rural, sigue una estructura común que indica un intercambio de plantillas o una imitación de técnicas exitosas entre diferentes grupos.

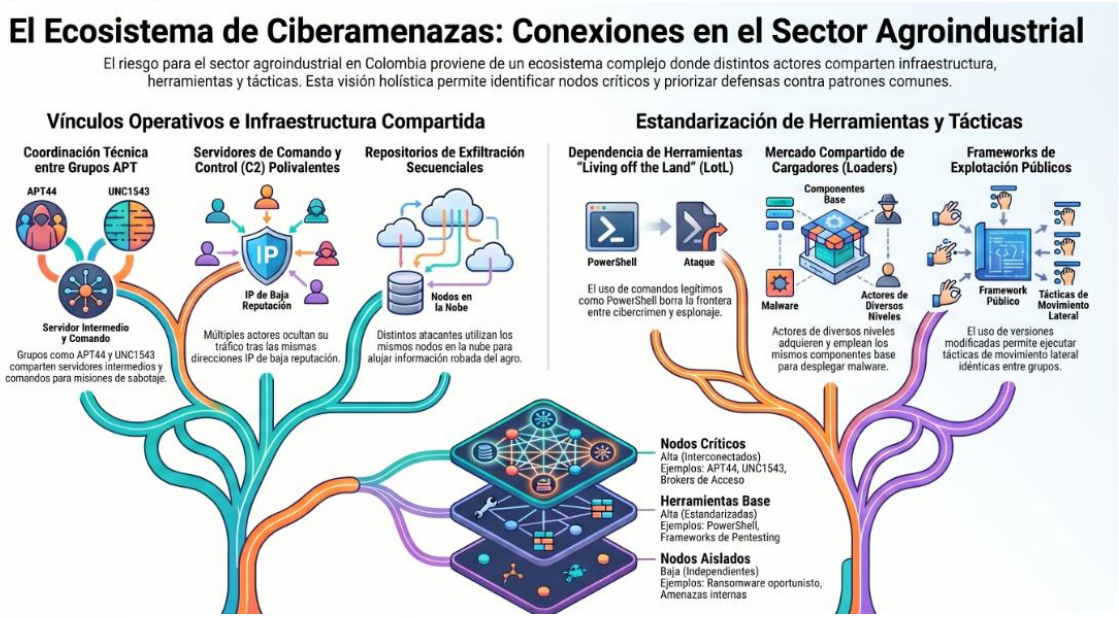
Posibles Colaboraciones o Vínculos

- Mercado de Acceso Inicial (Initial Access Brokers): Se sospecha que grupos como UNC3840 actúan como proveedores, obteniendo acceso inicial a redes agroindustriales para luego vender dicho acceso a grupos más especializados en espionaje (APTs) o extorsión (Ransomware).

- Vínculos por Motivación Geopolítica: La coincidencia en los tiempos de ataque y los objetivos seleccionados sugiere una posible alineación estratégica entre grupos APT, donde un actor realiza el sabotaje operativo mientras otro se encarga de la exfiltración de inteligencia económica.

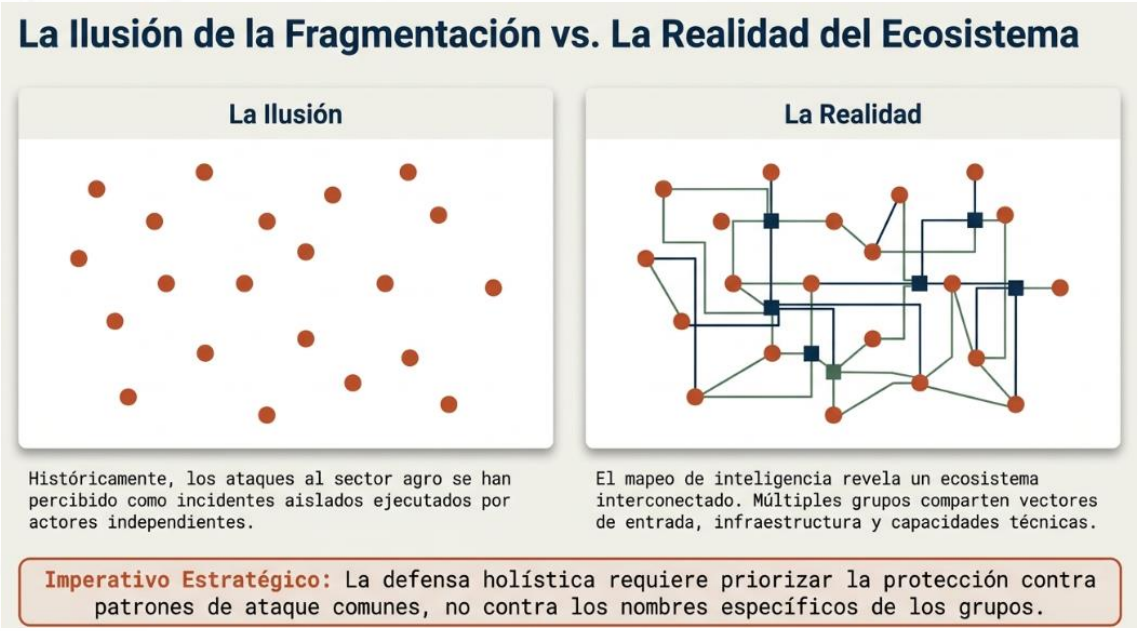
- Adopción de Frameworks de Explotación Públicos: El uso compartido de frameworks de pruebas de penetración modificados permite que grupos con diferentes niveles de habilidad técnica ejecuten ataques con una eficacia similar, borrando las líneas de distinción entre el cibercrimen común y el espionaje estatal.

Visualización de Relaciones



La visualización de las conexiones entre los distintos actores de amenazas permite comprender que el riesgo para el sector agroindustrial no es fragmentado, sino que forma parte de un ecosistema de ciberinteligencia complejo. Al mapear estas relaciones, se identifican nodos críticos donde la infraestructura y las herramientas se entrelazan, revelando que múltiples grupos pueden utilizar vectores de entrada idénticos o compartir capacidades técnicas para alcanzar sus objetivos. Esta visión holística es fundamental para que las organizaciones del agro en Colombia prioricen sus defensas no contra un "nombre" de grupo, sino contra los patrones de ataque que son comunes a toda la red de adversarios.

Relaciones directas documentadas:



- **Interacción entre APT44 y UNC1543:** Se ha documentado el uso de infraestructuras de salto y servidores intermedios donde la telemetría muestra el paso de comandos asociados a ambos grupos. Esto sugiere una posible coordinación técnica o una relación de subordinación operativa en misiones de sabotaje.

- **Dependencia de APT19 de Brokers de Acceso:** Existe una relación directa entre grupos de intrusión dirigida y actores APT, donde los primeros realizan el compromiso inicial a gran escala y los segundos toman el control de las víctimas de alto valor (como directivos de gremios agrícolas) para realizar espionaje a largo plazo.

- **Vínculos entre Campañas de Suplantación:** Se han identificado dominios de phishing que utilizan certificados digitales idénticos a los empleados en operaciones confirmadas de **APT44**, indicando que el proceso de creación de señuelos está centralizado o sigue un manual de procedimientos compartido.

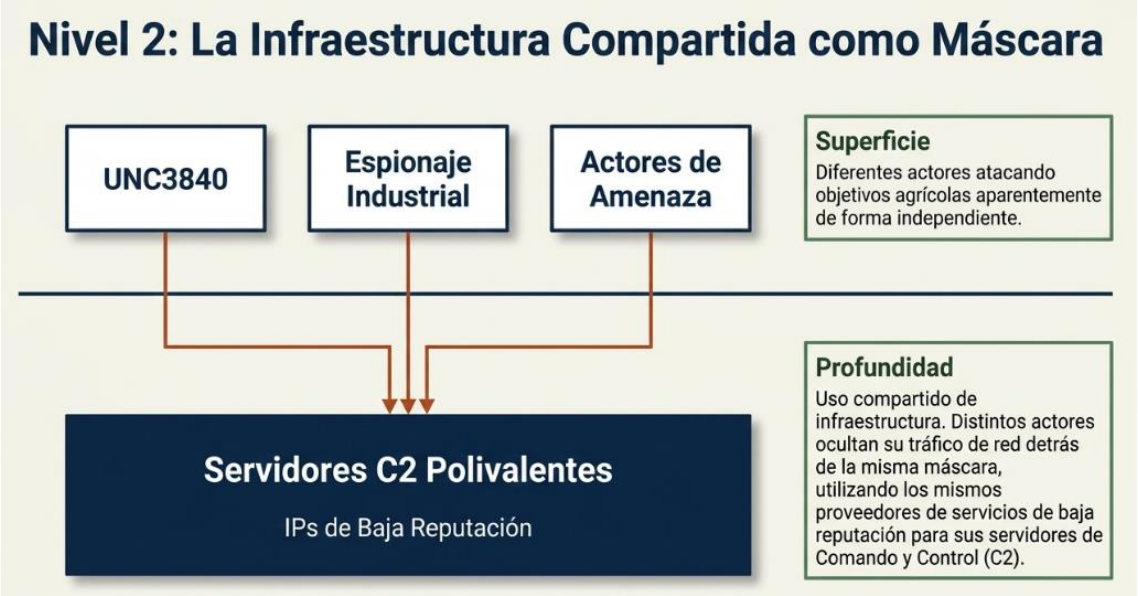
Relaciones por infraestructura compartida

- **Uso de Servidores de Comando y Control (C2) Polivalentes:** Grupos como **UNC3840** y actores vinculados al espionaje industrial comparten el uso de direcciones IP alojadas en proveedores de servicios de baja reputación, lo que permite a diferentes actores ocultar su tráfico tras una misma máscara de red.

- **Registros de DNS y Patrones de Nomenclatura:** La identificación de dominios como white-check-security.tools y core1draw.com muestra una consistencia en el uso de los mismos registradores y servicios de protección de privacidad por parte de diferentes grupos de amenazas.

- **Nodos de Exfiltración de Datos:** Se han detectado repositorios de almacenamiento en la nube comprometidos que han sido utilizados secuencialmente por distintos actores para alojar temporalmente información robada de diversas entidades del sector agro.

Relaciones por herramientas comunes

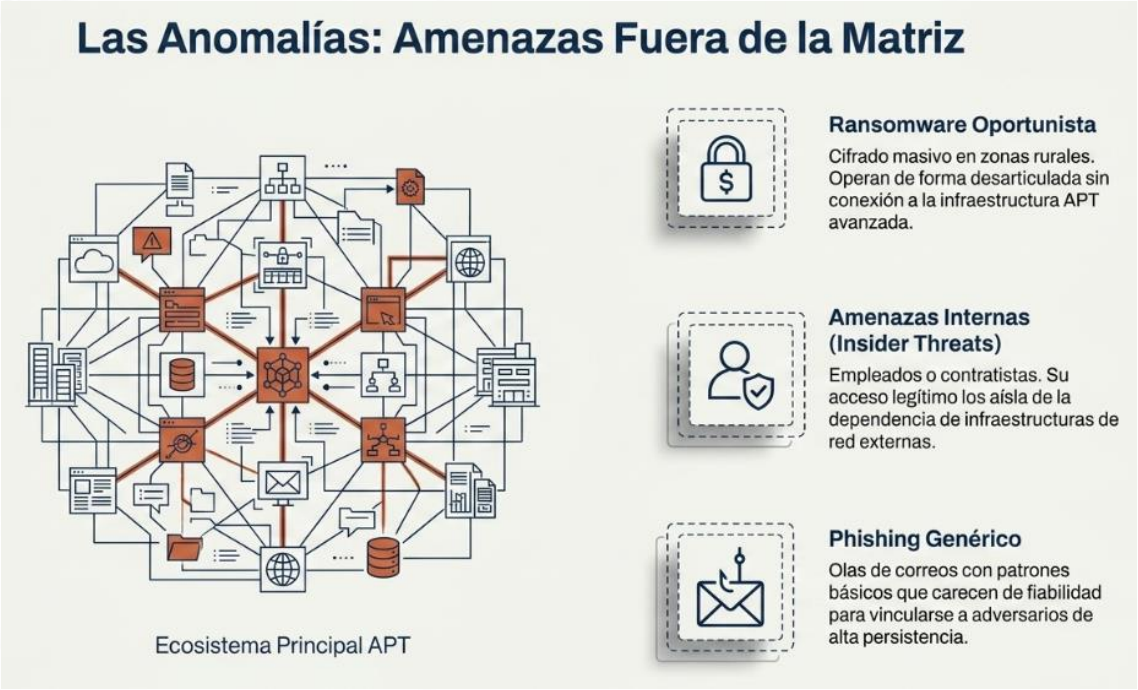


- Estandarización de Cargadores (Loaders): El uso de scripts de carga similares para desplegar diferentes tipos de malware indica un mercado compartido de herramientas de desarrollo donde actores de diversos niveles de sofisticación adquieren los mismos componentes base.

- Adopción Transversal de Herramientas LotL: La dependencia de herramientas de administración legítimas (como comandos de red y PowerShell) es un rasgo común entre todos los grupos analizados, lo que borra las fronteras técnicas entre un ataque de cibercrimen financiero y uno de espionaje estatal.

- Frameworks de Explotación Públicos: El empleo de versiones modificadas de frameworks de pruebas de penetración permite que múltiples actores ejecuten tácticas de movimiento lateral idénticas, dificultando la atribución específica a un solo grupo.

Nodos aislados o con baja correlación:



- Actores de Ransomware Oportunistas: Algunos grupos que realizan ataques masivos de cifrado de datos en zonas rurales muestran poca o ninguna conexión con la infraestructura avanzada de los grupos APT, operando de forma totalmente independiente y desarticulada.

- Amenazas Internas (Insider Threats): El riesgo derivado de empleados o contratistas con acceso legítimo permanece como un nodo aislado, ya que sus acciones no suelen depender de la infraestructura de red externa utilizada por los grupos de amenazas externos.

- Campañas de Phishing Genéricas: Ciertas olas de correos maliciosos detectadas en el sector muestran patrones tan básicos y genéricos que no pueden ser vinculados con fiabilidad a ninguno de los adversarios de alta persistencia identificados en este informe.

RECOMENDACIONES ESTRATÉGICAS

El fortalecimiento de la postura de seguridad para el sector agroindustrial requiere un enfoque integral que trascienda la protección perimetral básica. La estrategia debe centrarse en la creación de una arquitectura de defensa en profundidad que reconozca la interdependencia entre los sistemas administrativos y las tecnologías de operación en campo. Ante la presencia de actores con alta capacidad de persistencia, las recomendaciones aquí presentadas buscan elevar el costo operativo para el atacante y reducir drásticamente la ventana de oportunidad para la exfiltración de datos estratégicos o el sabotaje de la producción nacional.

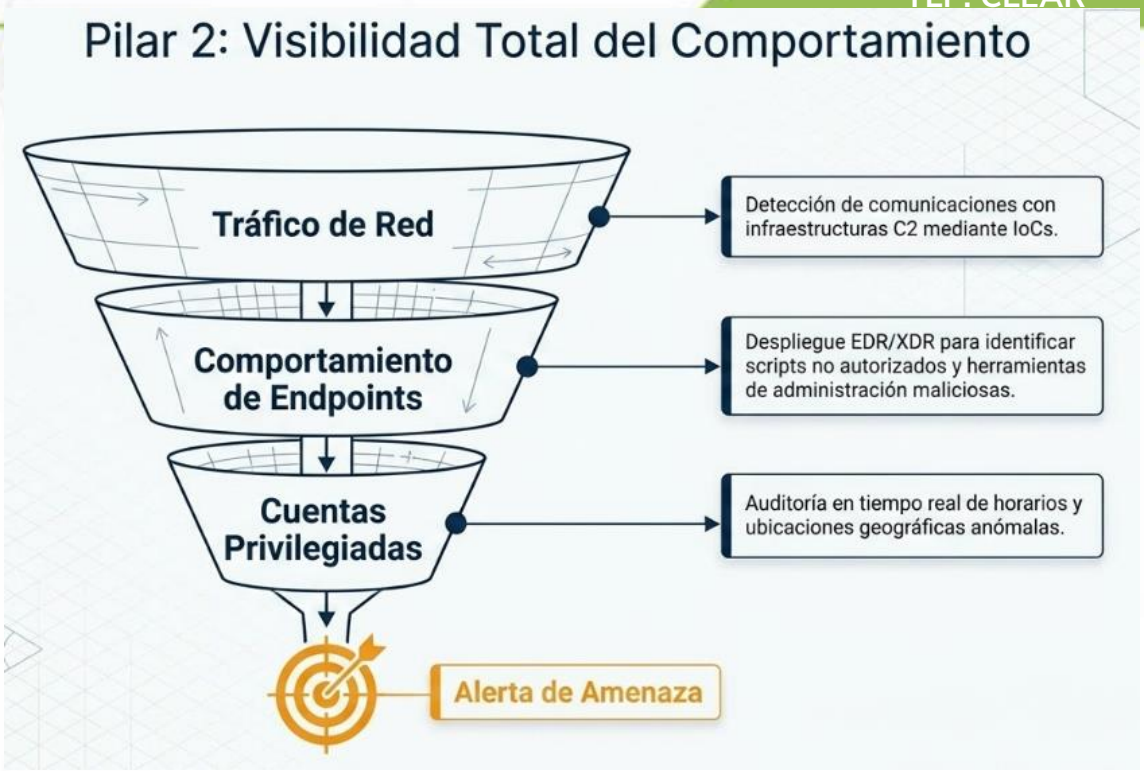
Recomendaciones de Mitigación Técnica

Para reducir la superficie de exposición, es fundamental implementar controles que limiten la capacidad de movimiento de los adversarios y protejan los activos críticos de la infraestructura productiva.

- **Segmentación Estricta IT/OT:** Establecer firewalls industriales y zonas desmilitarizadas (DMZ) para aislar las redes de control de riego, silos y sensores de las redes corporativas de oficina.
- **Implementación de Autenticación Multifactor (MFA):** Exigir MFA en todos los servicios expuestos a internet, especialmente en plataformas de gestión logística, correos institucionales y accesos remotos (VPN/RDP).
- **Gestión de Vulnerabilidades Priorizada:** Ejecutar ciclos de parcheo mensuales enfocados en activos críticos, priorizando aquellos que presentan vulnerabilidades conocidas y explotadas según la telemetría de inteligencia.
- **Hardening de Estaciones de Control:** Aplicar configuraciones de seguridad robustas en las terminales que operan maquinaria industrial, deshabilitando puertos USB innecesarios y servicios no críticos.

Recomendaciones de Detección y Monitoreo

La visibilidad es la clave para identificar a los adversarios antes de que cumplan sus objetivos. Se deben establecer capacidades de vigilancia que cubran tanto el tráfico de red como el comportamiento de los endpoints.



- **Despliegue de Soluciones EDR/XDR:** Implementar herramientas de detección y respuesta en puntos finales para identificar comportamientos anómalos, como la ejecución de scripts no autorizados o el uso de herramientas de administración con fines maliciosos.
- **Monitoreo de Tráfico hacia C2:** Configurar reglas de detección basadas en los IoCs proporcionados (IPs y dominios) para alertar sobre cualquier intento de comunicación con infraestructuras de comando y control conocidas.
- **Auditoría de Cuentas Privilegiadas:** Supervisar en tiempo real el uso de credenciales de administrador, buscando patrones de inicio de sesión inusuales en horarios o ubicaciones geográficas no habituales.

Recomendaciones de Resiliencia Operativa

La resiliencia implica la capacidad de mantener las operaciones mínimas esenciales incluso bajo un estado de compromiso cibernético activo.

- **Estrategia de Respaldos Offline:** Mantener copias de seguridad de datos críticos (fórmulas biotecnológicas, bases de datos de exportación) fuera de línea o en entornos inmutables para mitigar ataques de ransomware.
- **Modos de Operación Manual:** Asegurar que los sistemas de control industrial (riego, clima, procesamiento) cuenten con procedimientos validados para operar de forma manual en caso de una caída total de los sistemas digitales.
- **Planes de Continuidad del Negocio (BCP):** Desarrollar y documentar protocolos específicos para la cadena de suministro que permitan gestionar la logística de productos perecederos ante una indisponibilidad de los sistemas IT.

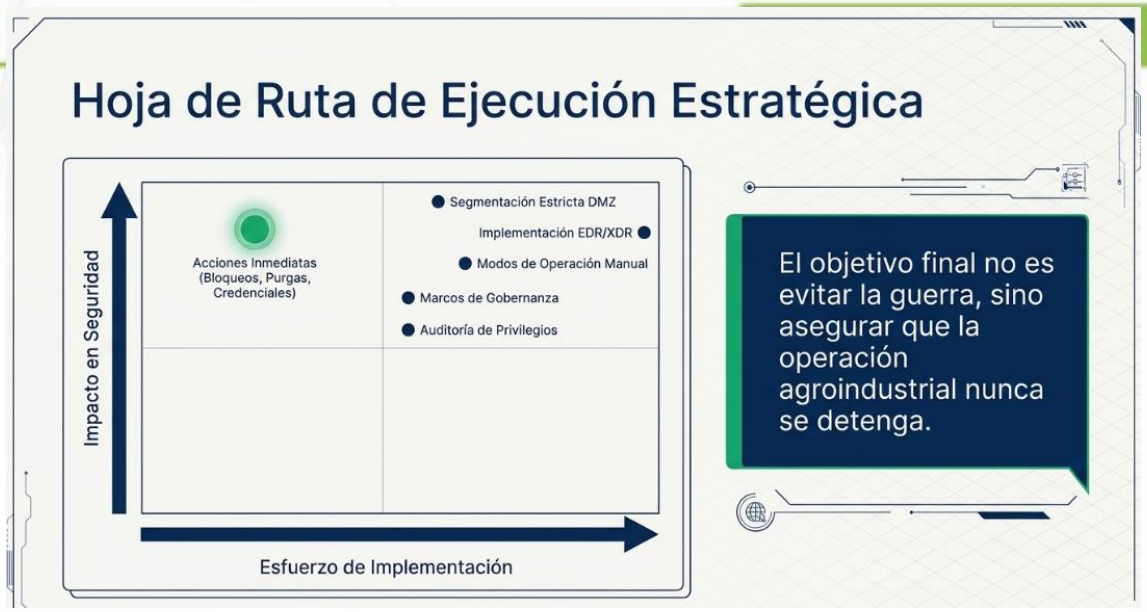
Recomendaciones de Gobernanza

La seguridad digital debe ser integrada en la estructura de toma de decisiones de las organizaciones agroindustriales como un riesgo de negocio y no solo técnico.

- **Adopción de Marcos de Referencia:** Alinear la gestión de ciberseguridad con estándares internacionales (como NIST o ISO 27001) adaptados a la realidad de la infraestructura crítica nacional.
- **Gestión de Riesgos de Terceros:** Establecer cláusulas de ciberseguridad en los contratos con proveedores de tecnología y logística, exigiendo niveles mínimos de protección para evitar ataques por cadena de suministro.
- **Cultura de Seguridad en el Campo:** Implementar programas de concientización para operarios y técnicos sobre los riesgos de la ingeniería social y el manejo seguro de dispositivos móviles en zonas de producción.

Preparación ante Incidentes

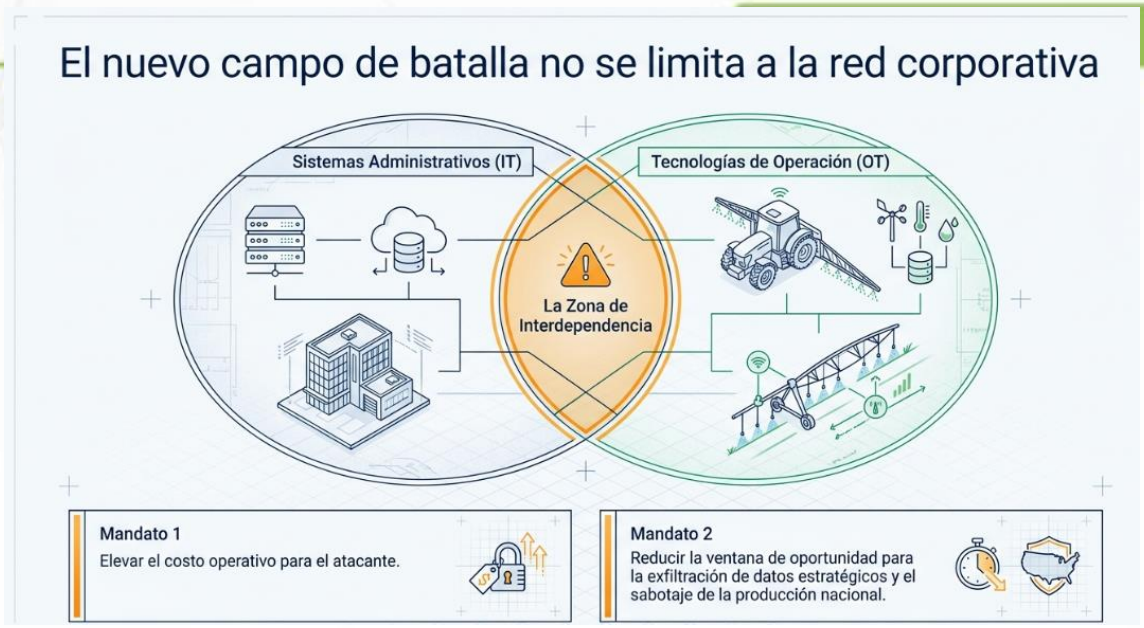
Estar preparados para lo inevitable reduce el impacto reputacional y económico de un ataque exitoso.



- **Desarrollo de Playbooks Específicos:** Crear guías de respuesta ante incidentes para escenarios de ransomware, fuga de información y sabotaje de sistemas OT.
- **Ejercicios de Simulación (Tabletop):** Realizar simulacros periódicos con la alta gerencia y los equipos técnicos para validar la efectividad de los planes de respuesta y la cadena de mando.
- **Establecimiento de Alianzas de Respuesta:** Mantener canales de comunicación activos con autoridades nacionales y CSIRTs sectoriales para el intercambio rápido de información durante una crisis.

Acciones Inmediatas (Quick Wins)

Estas acciones pueden ejecutarse en el corto plazo con recursos existentes para mejorar la postura de seguridad de forma instantánea.



- **Bloqueo de IoCs Identificados:** Integrar de inmediato la lista de IPs, dominios y hashes detallados en este informe en las listas de bloqueo de firewalls y soluciones de seguridad.
- **Revisión de Accesos de Ex-empleados:** Realizar una purga de cuentas activas de personal que ya no pertenece a la organización, especialmente aquellas con privilegios de administración.
- **Deshabilitación de Macros y Scripts:** Restringir la ejecución automática de macros en documentos de oficina y scripts de PowerShell en estaciones de trabajo no técnicas.
- **Cambio de Credenciales por Defecto:** Asegurar que ningún dispositivo IoT o sensor de campo mantenga las contraseñas configuradas por el fabricante.

CONCLUSIONES

- **Elevación del Perfil de Amenaza:** El sector agroindustrial ha dejado de ser un objetivo secundario para convertirse en un frente crítico de seguridad nacional. La presencia confirmada de actores de clase mundial como **APT44 (Sandworm)** y **APT19** indica que la infraestructura productiva colombiana está bajo la mira de operaciones de espionaje y sabotaje con capacidades de nivel estatal.

- **Convergencia IT/OT como Punto Crítico de Falla:** La modernización tecnológica del campo ha creado una dependencia total de sistemas interconectados. La falta de una segmentación estricta entre las redes administrativas y los sistemas de control de campo (riego, silos, procesamiento) representa la mayor vulnerabilidad, permitiendo que ataques convencionales de oficina escalen hasta detener la producción física.

- **El Dato como Activo Estratégico en Riesgo:** Existe un interés sistemático por parte de los adversarios en el robo de propiedad intelectual biotecnológica, patentes de semillas y estrategias comerciales. Este tipo de exfiltración silenciosa, detectada en las tendencias de incidentes "Grave" y "Muy Grave", impacta directamente en la competitividad y la soberanía alimentaria del país a largo plazo.

- **Profesionalización del Cibercrimen mediante la Cadena de Suministro:** Los actores de amenazas están utilizando a proveedores de tecnología y logística como puente de entrada (Supply Chain Attack). Grupos como **UNC3840** actúan como facilitadores, comprometiendo primero el ecosistema de servicios del agro para luego otorgar acceso profundo a redes institucionales de alto valor.

- **Persistencia y Evolución de Tácticas:** El análisis de los TTPs mapeados a MITRE ATT&CK demuestra que los atacantes están perfeccionando el uso de herramientas legítimas del sistema ("Living off the Land") para evadir defensas. Esta evolución técnica reduce la efectividad de las soluciones de seguridad tradicionales basadas únicamente en firmas, obligando a adoptar modelos de detección por comportamiento.

- **Urgencia de una Cultura de Resiliencia Proactiva:** El historial de incidentes registrados entre 2023 y 2026 evidencia que el sector aún opera bajo una postura reactiva. La conclusión estratégica definitiva es la necesidad de transicionar hacia una gobernanza de ciberseguridad que integre planes de continuidad operativa manual y una vigilancia constante de indicadores de compromiso (IoCs) específicos para la geografía y el contexto colombiano.

GLOSARIO

TLP: CLEAR

Conceptos de Inteligencia y Amenazas

- **Amenaza Persistente Avanzada (APT):** Grupos de atacantes altamente capacitados y con grandes recursos (frecuentemente respaldados por estados) que realizan campañas de intrusión prolongadas y dirigidas con objetivos específicos, como el espionaje industrial.
- **Indicadores de Compromiso (IoCs):** Evidencias digitales (como una dirección IP, un dominio o una firma de archivo) que indican con un alto nivel de confianza que un sistema ha sido vulnerado.
- **Tácticas, Técnicas y Procedimientos (TTPs):** Marco que describe el "cómo" actúan los atacantes. Las tácticas son los objetivos (ej. Acceso Inicial), las técnicas son los métodos (ej. Phishing) y los procedimientos son la ejecución específica.
- **Superficie de Ataque:** La suma total de todos los puntos de exposición (software, hardware, redes y usuarios) por los cuales un atacante podría intentar ingresar a una organización.
- **Cadena de Ataque (Kill Chain):** Modelo que describe las fases de un ciberataque, desde el reconocimiento inicial hasta el cumplimiento de los objetivos (como el robo de datos o el sabotaje).
- **Initial Access Broker (IAB):** Actores que se especializan en obtener acceso a redes corporativas para luego vender ese acceso a otros grupos de mayor peligrosidad, como operadores de ransomware.

Infraestructura y Redes

- **Tecnología de Operación (OT):** Hardware y software diseñado para detectar o causar cambios mediante el monitoreo y control directo de dispositivos físicos, como sistemas de riego automatizados o maquinaria de procesamiento.
- **Sistemas de Control Industrial (ICS):** Segmento de la tecnología de operación que incluye los sistemas utilizados para monitorear y controlar procesos industriales y técnicos en el campo.
- **Controlador Lógico Programable (PLC):** Computadora robustecida utilizada para la automatización de procesos electromecánicos, fundamentales en la gestión de silos, invernaderos y plantas de beneficio.
- **Segmentación de Red:** Práctica de dividir una red informática en subredes más pequeñas para mejorar el rendimiento y, sobre todo, para evitar que un atacante se mueva lateralmente desde una zona administrativa hacia una zona de producción.

- **Air-gap:** Medida de seguridad que consiste en asegurar que una red informática crítica esté físicamente aislada de redes inseguras, como el internet público o la red de oficina.

Herramientas y Malware

- **Ransomware:** Tipo de malware que cifra los archivos de la víctima y exige un rescate económico para devolver el acceso, siendo una amenaza crítica para la continuidad operativa de la cadena de suministro.
- **Troyano de Acceso Remoto (RAT):** Malware que permite a un atacante tomar el control total de un sistema de forma remota, permitiendo el espionaje de documentos técnicos y comunicaciones.
- **Living off the Land (LotL):** Técnica de ataque que utiliza herramientas y archivos legítimos que ya están presentes en el sistema operativo para llevar a cabo actividades maliciosas, lo que dificulta su detección.
- **Phishing:** Técnica de ingeniería social que utiliza correos electrónicos fraudulentos para engañar a los empleados y obtener credenciales de acceso o instalar malware.
- **Web Shell:** Interfaz de comandos cargada de forma maliciosa en un servidor web que permite a los atacantes ejecutar órdenes en el servidor de forma persistente.

Sector

- **Infraestructura Crítica:** Activos, sistemas y redes, ya sean físicos o virtuales, que son tan vitales para el país que su incapacidad o destrucción tendría un impacto debilitante en la seguridad, la economía o la salud pública (ej. la producción de alimentos).
- **Ciberresiliencia:** Capacidad de una organización o sector para anticipar, resistir, recuperarse y adaptarse a condiciones adversas, ataques o compromisos en sus sistemas digitales.
- **Soberanía Alimentaria:** Derecho de los pueblos a definir sus propias políticas y estrategias sustentables de producción, distribución y consumo de alimentos; en este contexto, protegida contra el sabotaje digital.
- **Propiedad Intelectual Agroindustrial:** Activos intangibles como secuencias genéticas, fórmulas de agroquímicos y procesos de mejoramiento de cultivos que son objetivos primarios de espionaje.

- **Gobernanza de Ciberseguridad:** El marco de reglas, procesos y prácticas mediante el cual la alta dirección de una agroindustria asegura que los riesgos digitales sean gestionados de acuerdo con los objetivos del negocio.

COLCERT

El **ColCERT** tiene la misión de liderar y coordinar la gestión de incidentes, la identificación de vulnerabilidades, riesgos y amenazas contra la seguridad digital nacional. Actuamos como punto central de contacto y colaboración entre entidades públicas, privadas y la comunidad internacional, fortaleciendo la resiliencia del Estado mediante el intercambio de información, el desarrollo de capacidades, la difusión de lineamientos, la identificación de infraestructuras críticas y la promoción de una cultura de seguridad, a través de la cooperación nacional e internacional.

Más allá de la gestión ante amenazas, el **ColCERT** fortalece la seguridad digital del país mediante acciones de prevención, orientación y generación de capacidades dirigidas a entidades públicas, privadas y ciudadanía, contribuyendo a una transformación digital más segura y resiliente en Colombia.

Conéctate con el ColCERT

Reporte de incidentes:
csirtgob@mintic.gov.co
Entidades de Gobierno

contacto@colcert.gov.co
Privados

icc@colcert.gov.co
Temas de ICC

Sitio web
https://www.colcert.gov.co
Alertas y boletines

@colCERT

Línea directa:
+57 601 344 2222