TIC

INFORME DE TENDENCIAS

DE AMENAZAS CIBERNÉTICAS 2025

CONOCIMIENTO ESTRATÉGICO AL SERVICIO DE LA TRANSFORMACIÓN Y LA CONFIANZA DIGITAL EN COLOMBIA

COLCERT IN-20260401-01



¡Protégete en cada clic!

www.colcert.gov.co

COLCERT

TIC

PRÓLOGO:

En un entorno cada vez más digital, la ciberseguridad se consolida como un pilar fundamental para la confianza, la estabilidad institucional y el desarrollo del país. Colombia ha enfrentado un aumento en la frecuencia y sofisticación de los ciberataques, así como la evolución de amenazas impulsadas por tecnologías emergentes como la inteligencia artificial. Este informe 2025, elaborado por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT, en su rol como CERT nacional, presenta una mirada clara y basada en evidencia sobre las vulnerabilidades identificadas en el país en 2025, así como las principales tendencias y riesgos emergentes que se proyectan para 2026.

Carina Murcia
Ministra de Tecnologías de la Información y las Comunicaciones de Colombia 2026.

COORDINACIÓN Y DESARROLLO TÉCNICO DEL INFORME.

Carina Murcia
Ministra de Tecnologías de la Información y las Comunicaciones de Colombia 2026

Andrés López
Viceministro de Transformación Digital

Gloria Perdomo
Viceministra de Conectividad

Grupo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT

TIC

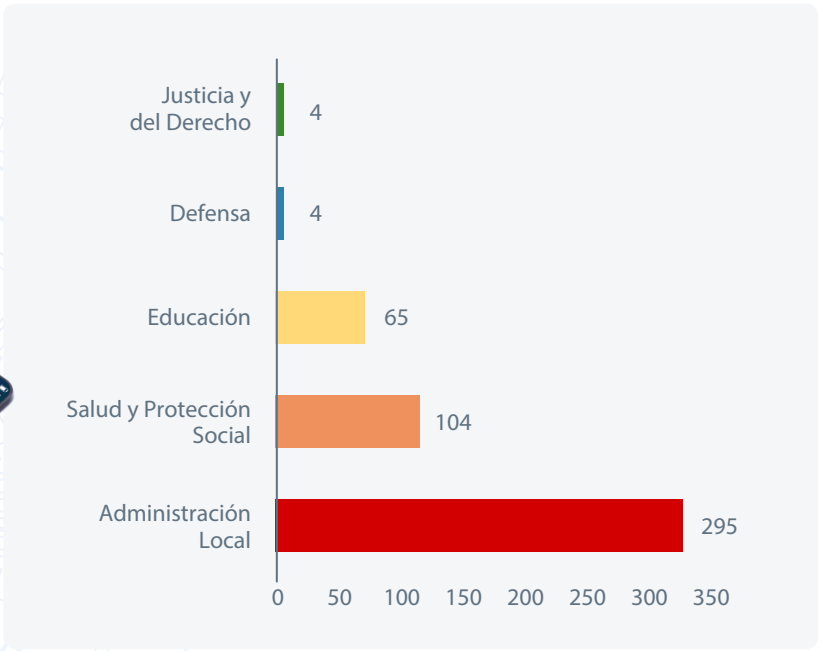
RESUMEN EJECUTIVO:

En el mapa digital de América Latina, Colombia ya no es un actor aislado, no por la innovación sino por la tendencia creciente del aumento de ciberataques, la sofisticación de los mismos y la selección de objetivos claves en sectores estratégicos. Por lo anterior, este informe tiene como propósito presentar tendencias, patrones y actores asociados a algunas de las amenazas más relevantes vistas en 2025, exponiendo las Amenazas Persistentes Avanzadas (Advanced Persistent Threats – APT) y las vulnerabilidades recurrentes en entidades públicas y privadas, a fin de orientar la toma de decisiones estratégicas, y lograr anticipar el escenario en 2026.

Fuente:
Construcción propia a partir de KVE de inf. compartida por CISA.

SECTORES MÁS AFECTADOS
EN COLOMBIA 2024-2025



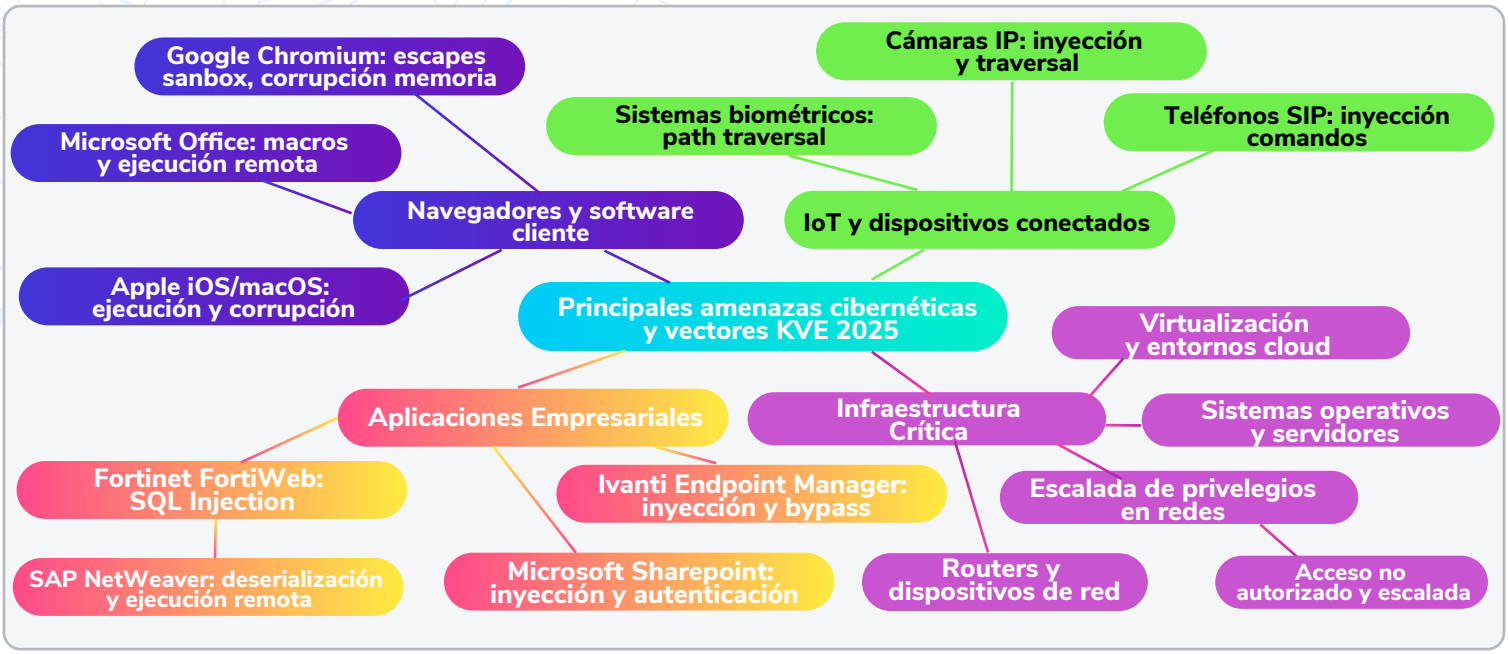


Fortinet FortiWeb: SQL Injection

Fuente: Construcción propia a partir de KVE de inf. compartida por CISA

- El sector más afectado por los incidentes reportados son las administraciones locales, lo cual probablemente esté relacionado con la falta de capacidades y conocimientos técnicos.
- La limitación y escasez de talento humano representa un obstáculo para el fortalecimiento de las capacidades de ciberseguridad en Colombia.
- La falta de continuidad de procesos o personal genera una brecha entre las políticas públicas y la ejecución de las mismas, afectando especialmente a sectores vulnerables como salud, administración o educación.
- En 2024-2025 **hubo** eventos de alto impacto **(ver anexo 1),** que han afectado principalmente al **sector gobierno, energía, salud, justicia,** entre otros. Estos eventos han buscado afectar la infraestructura crítica cibernética generando la interrupción del servicio, de actores públicos y privados.
- Es fundamental aumentar la inversión en ciberseguridad de forma sostenida y continua, no solo como una respuesta temporal, para proteger eficazmente la infraestructura crítica frente a amenazas cada vez más sofisticadas.

VULNERABILIDADES EXPLOTADAS CONOCIDAS
(KVE, POR SUS SIGLAS EN INGLÉS)



Fuente: Construcción propia a partir de KVE de inf. compartida por CISA

- El reporte de los **KVE** publicado por **CISA [3]** evidencia que en 2025 las principales vulnerabilidades explotadas se han enfocado en Infraestructura crítica, aplicaciones empresariales y dispositivos **IoT.**
- La tendencia global y vectores emergentes para 2025 proyecta que continue el Ransomware y la doble extorsión con modelos RaaS **(Ransomware as a Service),** afectando desde infraestructuras críticas hasta redes empresariales cloud, respaldos y servicios **SaaS.**
- La explotación de credenciales y evasión multifactor se posicionan cada vez más como ataques avanzados con robo de credenciales y compromisos prolongados de los sistemas.
- Las principales tendencias de amenazas se dan sobre, navegadores y software de cliente; **IoT;** infraestructura crítica, aplicaciones empresariales, servicios cloud, Escalada y compromiso local; así como la explotación de credenciales, tal como se evidencia en la gráfica.

- El Ataque a los servicios de **Cloud y APIs** tiende a incrementar con la explotación de configuraciones erróneas, inyección y acceso por cadenas de suministro, apuntando a **APIs** web, herramientas de backup y plataformas cloud, donde la seguridad perimetral es insuficiente.



TENDENCIAS REGIONALES

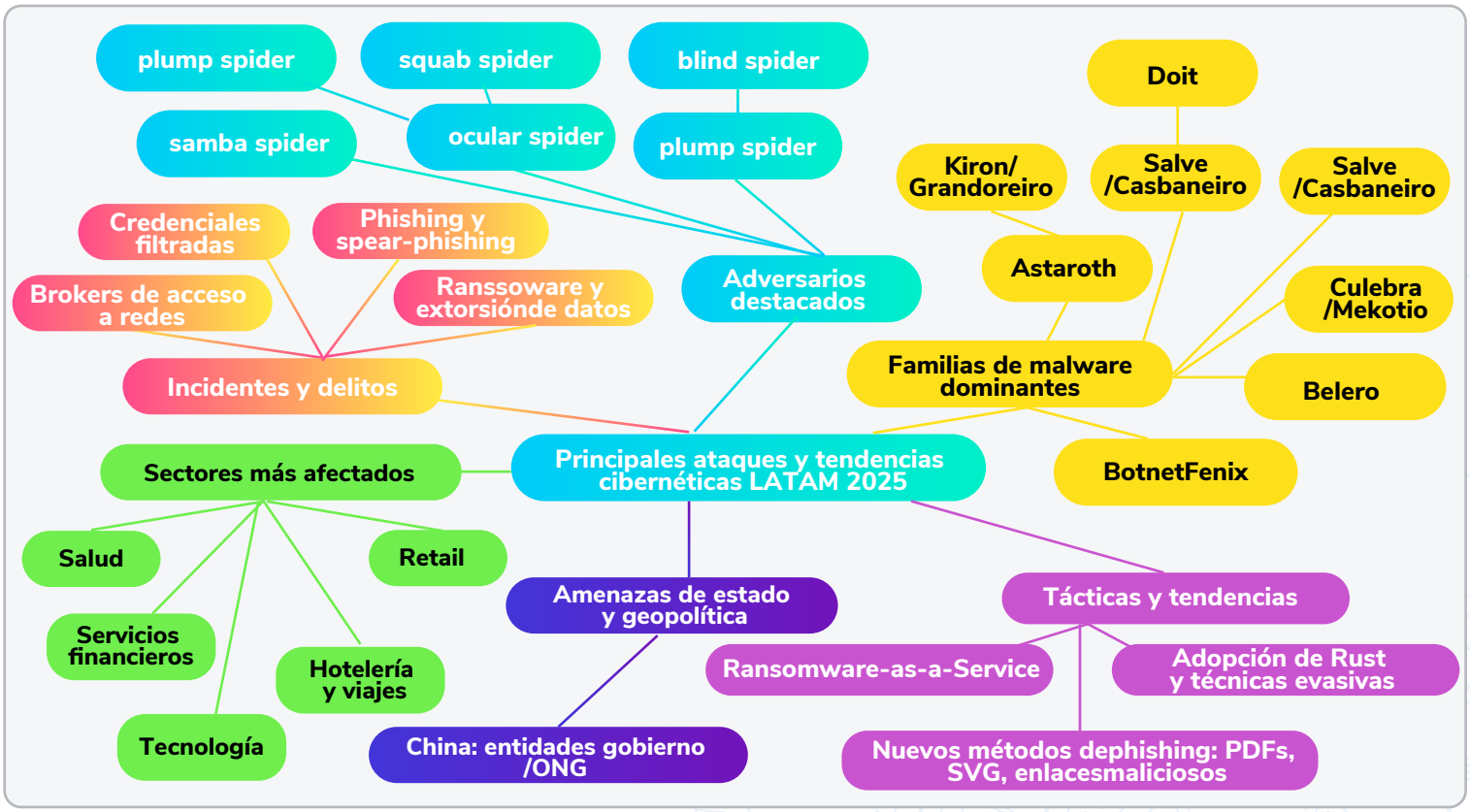
- El crecimiento del ransomware en América Latina se impulsó por la presencia y acción de estos actores, quienes presentan mayor actividad en estas amenazas en la región. Los actores de **OCULAR SPIDER, BLIND SPIDER, ODYSSEY SPIDER, PLUMP SPIDER, SAMBA SPIDER y SQUAB SPIDER [1].** En 2024, se documentaron 291 víctimas de ransomware y extorsión de datos en América Latina. En el caso de Colombia según Crowd Strike se reportaron más de 10 incidentes, situándose dentro de los seis países más afectados, detrás de Brasil, México y Argentina.

- Entre los principales malware recientes con operación en Colombia se encuentran Mispadu, Kiron **(Grandoreiro),** Caiman, Astaroth, Culebra **(Mekotio),** Salve **(Casbaneiro),** Doit, BotnetFenix y Belero. Destaca la adopción de nuevos lenguajes de programación como Rust para evadir defensa y dificultar la atribución **(CrowdStrike, 2025, p. 25) [1].**

- El aumento de ataques impulsados por IA probablemente se intensifique con las amenazas con malware adaptativo, phishing automatizado y falsificaciones profundas **(Deep Fake). [1].**



- Durante 2024, Colombia registró un número significativo de credenciales filtradas en incidentes, lo que sugiere la magnitud del reto: “A lo largo del 2024, **inteligencia de CrowdStrike** recuperó más de 1,000 millones de credenciales pertenecientes a personas y organizaciones con sede en LATAM... México, Argentina, Colombia y Perú también registraron un elevado número de credenciales filtradas” **(CrowdStrike, 2025, p. 23).**



Fuente: Construcción propia a partir de Crowd Strike (2025).

TENDENCIAS REGIONALES:

- La creciente transformación digital no ha sido acompañada por la inversión en ciberseguridad en todos los niveles y entidades, exponiendo infraestructuras críticas en países como Colombia a intrusiones cada vez más sofisticadas.
- Los actores con vínculo con China, Corea del Norte y Rusia han tenido a Colombia como objetivo secundario, aunque en menor escala que los grupos de cibercrimen. Sin embargo, los principales APT identificadas a nivel mundial provienen de algunos de estos países.

- Existe un riesgo elevado sobre la cadena de suministro y servicios SaaS, un ejemplo de ello fue la brecha de Bankingly (2024) que afectó a múltiples bancos de LATAM debido a fallos en configuraciones en la nube, lo que también podría impactar a entidades colombianas que dependan de servicios compartidos.

- Con base en la información disponible se anticipa una creciente tendencia de amenazas enfocadas al robo de credenciales, ransomware y campañas de phishing, así como la evolución de malware que desarrolle nuevas técnicas de evasión, tal como se expresa en el gráfico donde se exponen las principales tendencias, actores destacados y los sectores más afectados.

ANÁLISIS DE INFRAESTRUCTURA CRÍTICA CIBERNÉTICA:

- Durante el estudio se encontró que la tendencia de afectaciones sobre infraestructura crítica de los Estados se dirige a los sectores de Gobierno, Defensa, Transporte, Comunicaciones, industria/manufactura, Salud, Educación, Finanzas y el Espacio. Con base en esto es de especial relevancia identificar y comprender como los sistemas interconectados pueden afectar al público.

- Para 2025-2026, Colombia probablemente presente un panorama donde múltiples sectores de infraestructura crítica enfrenten un aumento sostenido de ataques complejos **(ransomware, ICS, APT, phishing).** Las amenazas provienen de cibercrimen, hacktivismo y actores estatales, por lo anterior, fortalecer los sistemas y pasar a una defensa proactiva es fundamental para anticipar las afectaciones.

- Es claro que detrás de las afectaciones hay una motivación financiera y de extorsión, aunque también en la actual coyuntura, es necesario fortalecer las capacidades para evitar la disrupción institucional con impacto en la gobernanza y la confianza tanto en las elecciones como en las acciones institucionales.





Fuente: Construcción propia a partir de Crowd Strike (2025).

Análisis

- En Colombia hay multiplicidad de actores que operan bajo diversas tácticas que utilizan malware y ransomware para afectar hospitales o lanzar campañas para espiar el Estado, tal es el caso del **APT-C36** O Blind Eagle **(Ver anexo 2).** Estos actores han enfocado sus acciones sobre la administración local, salud, educación, justica, defensa y servicios públicos lo que genera una afectación directa al ciudadano **(Ver anexo 1).** Estos ataques recientes o de impacto como lo fue el de **IFX** o el reciente sobre la justicia penal militar, lo que impacta los servicios en línea, llevando a la suspensión de procesos y generando preocupaciones en torno a la confianza institucional.



- Por lo anterior se requiere una ciberresiliencia ampliada con capacidades de detección avanzada, planes de contingencia y un back up robusto.

- El crecimiento de la IA es clave no solo para los atacantes sino para el desarrollo de respuestas autónomas y de análisis en tiempo real, por lo que puede ser una respuesta a la tendencia de ataques presentada en LATAM y el mundo.

- Fortalecer la seguridad en la nube y la arquitectura de Zero Trust, va de la mano con la gestión correcta de la infraestructura crítica, tanto su identificación como la colaboración público-privada para integrar y coordinar respuestas ante posibles incidentes.

- El análisis de los últimos dos años de la gestión de incidentes de seguridad digital a nivel nacional revela que, durante el 2024, el ColCERT gestionó un total de 1,427 incidentes, una cifra que disminuyó a 697 en 2025, lo que representa una reducción del 48.84%. La disminución no debe interpretarse como una reducción en la actividad de los adversarios, sino como un aumento en la resiliencia del ecosistema digital colombiano.

- El año 2025 representa un antes y un después en la historia de la ciberdefensa en Colombia. Hemos superado con las capacidades operativas de años anteriores, transformando una gestión que en 2023 era centralizada y limitada, en una operación de cobertura nacional total. La transformación digital de ColCERT ha permitido pasar de un modelo de Gestión Centralizada a una estrategia de Cobertura Total País.

- Los indicadores de gestión comparativos entre 2023 y 2025 evidencian una explosión en la capacidad técnica y operativa sin precedentes. Como evidencia la siguiente gráfica de evolución, el crecimiento institucional y el aumento de la capacidad técnica nos han permitido iluminar el mapa de riesgos de los 32 departamentos del país.

- Se identificaron patrones temporales consistentes, en cada año, en el mes de agosto se registró el pico más alto de actividad, con 228 incidentes en 2024 y 115 incidentes en 2025. El trimestre que comprende los meses de julio, agosto y septiembre concentra consistentemente un volumen elevado de reportes, sugiriendo un período de mayor riesgo que podría correlacionarse con ciclos operativos o administrativos tanto en el sector público como en el privado. Este comportamiento ofrece una oportunidad para la planificación proactiva, permitiendo intensificar las campañas de concienciación y reforzar la vigilancia en los meses de mayor afectación.

- La comprensión de la naturaleza de las amenazas es fundamental para diseñar defensas efectivas, el análisis de los incidentes gestionados durante el 2024 y el 2025 revela que el panorama de amenazas está dominado por una categoría principal. El fraude se mantiene como la clase de incidente más relevante, representando un 87.29% del total de incidentes gestionados entre 2024 y 2025. Esta categoría es impulsada principalmente por dos tipos de ataques: el phishing, con 835 casos, y el uso no autorizado de recursos (principalmente compromiso de correos electrónicos), con 784 casos. La persistencia de estas tácticas de ingeniería social marca una brecha significativa en la concienciación y la higiene digital de los usuarios.

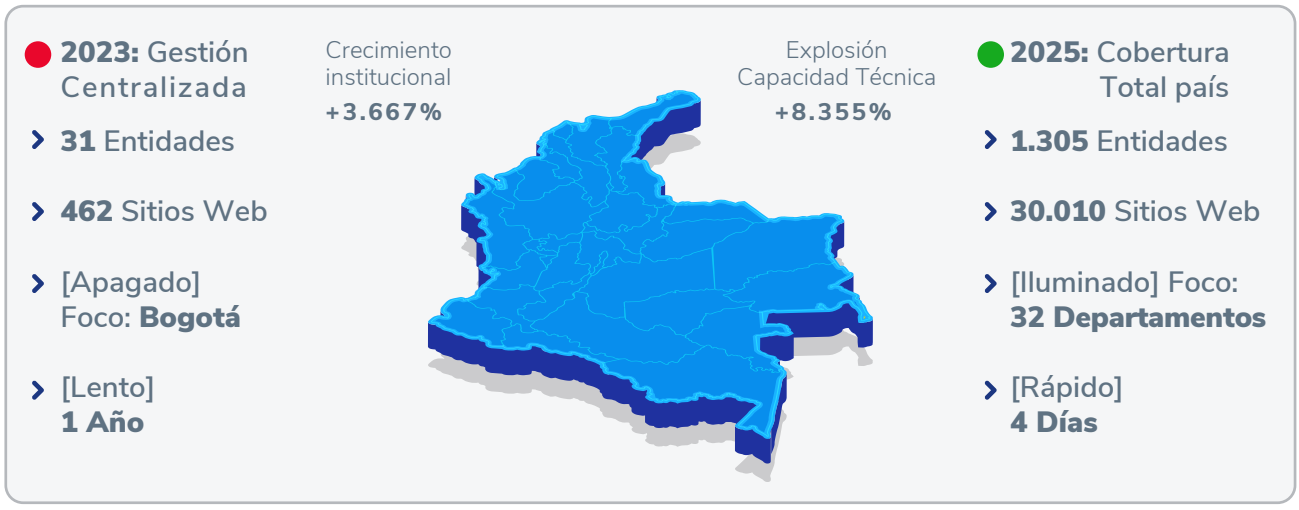
SITUACIÓN ACTUAL DE VULNERABILIDADES EN COLOMBIA 2025

***El salto cuántico:** De la gestión centralizada a la cobertura total*

El año 2025 representa un antes y un después en la historia de la ciberdefensa en Colombia. Hemos superado con las capacidades operativas de años anteriores, transformando una gestión que en 2023 era centralizada y limitada, en una operación de cobertura nacional total. La transformación digital de **ColCERT** ha permitido pasar de un modelo de Gestión Centralizada a una estrategia de Cobertura Total País.

Los indicadores de gestión comparativos entre 2023 y 2025 evidencian una explosión en la capacidad técnica y operativa sin precedentes. Como evidencia la siguiente gráfica de evolución, el crecimiento institucional y el aumento de la capacidad técnica nos han permitido iluminar el mapa de riesgos de los 32 departamentos del país:

Evolución de la Capacidad Defensiva 2023-2025



[Gráfica 1: Comparativo de evolución. Se destaca el paso de monitorear 31 entidades en 2023 a 1.305 en 2025, y la reducción drástica en los tiempos de respuesta de 1 año a 4 días.

Este logro operativo significa que hoy ColCERT tiene una velocidad de respuesta sin precedentes, pasando de ciclos de análisis de un año a tan solo 4 días.

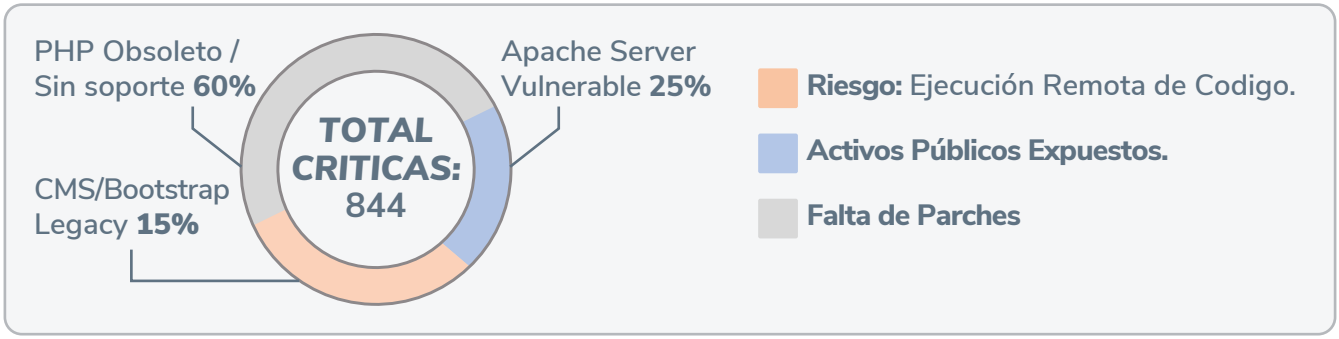
RADIOGRAFÍA DE LA VULNERABILIDAD CRÍTICA:

OBSOLESCENCIA TECNOLÓGICA

El escaneo de vulnerabilidades críticas sobre la muestra de activos territoriales y nacionales revela que el 85% de los riesgos críticos no provienen de ataques de día cero, sino de Deuda Técnica y Obsolescencia (End of Life - EOL).

Se han identificado tres vectores de ataque predominantes que comprometen la disponibilidad e integridad de los portales de gobierno (gov.co):

- **Vector 1:** Lenguajes de Programación sin Soporte. Se identificó una prevalencia alarmante de PHP en versiones no soportadas (o versiones antiguas 8.1.x y 8.2.x sin parchar). Impacto: Al no recibir actualizaciones de seguridad, estos servidores son vulnerables a ejecuciones de código arbitrario.
- **Vector 2:** Infraestructura Web Desactualizada **(Apache HTTP Server).** Persistencia de versiones de Apache 2.4.x (inferiores a 2.4.60 y 2.4.56). Impacto: Estas versiones contienen vulnerabilidades conocidas que permiten a atacantes eludir restricciones de acceso o realizar denegación de servicio **(DoS).**
- **Vector 3: : Frameworks y CMS Vulnerables.** Se detectaron componentes críticos obsoletos en librerías de interfaz y gestión de contenido, específicamente Bootstrap (Unsupported), Moodle (versiones < 4.1.16) y Drupal. Impacto: Esto facilita ataques de Cross-Site Scripting (XSS) y compromiso de plataformas educativas y de atención al ciudadano. La recurrencia de la vulnerabilidad "Unsupported Version" en los logs indica que las entidades no están gestionando el ciclo de vida del software. Los atacantes no necesitan herramientas sofisticadas; solo requieren scripts públicos que exploten fallos ya corregidos hace años por los fabricantes.



Gráfica 2: Distribución de Vulnerabilidades Críticas (Fuente: Tenable). El análisis táctico revela que el 85% del riesgo crítico en las 1.256 entidades proviene de software obsoleto y deuda técnica, siendo el uso de PHP sin soporte (60%) y servidores Apache vulnerables (25%) los principales vectores de ataque identificados, facilitando la ejecución remota de código.

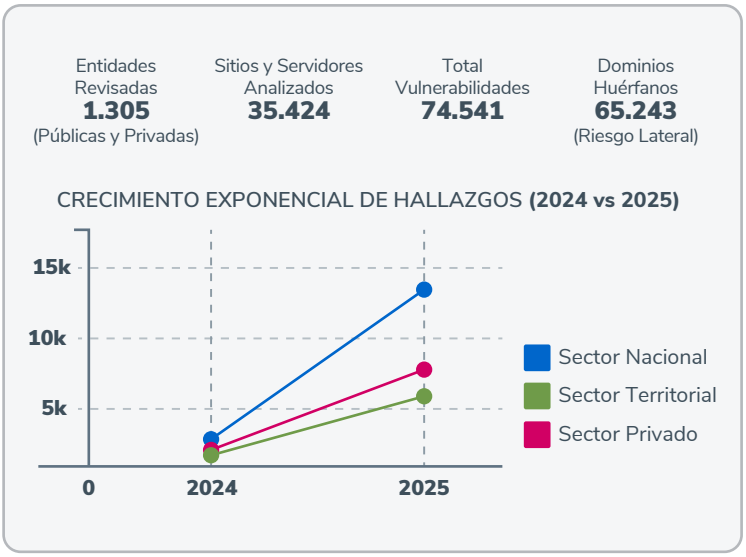
CIFRAS CONSOLIDADAS DE GESTIÓN:

Se revisaron un total de 1.305 entidades (públicas y privadas) y se analizaron 35.424 sitios web y servidores a nivel nacional. En total, se identificaron 74.541 vulnerabilidades en la infraestructura tecnológica del país.

Se detectaron 65.243 dominios abandonados o sin gestión, representando una superficie de riesgo latente. Del universo total de hallazgos, la prioridad de ColCERT se centra en las vulnerabilidades que comprometen la integridad inmediata de los sistemas:

- **CRÍTICAS:** 844. (Riesgo inminente).
- **MEDIAS:** 32.574.
- **ALTAS:** 26.560. (Riesgo elevado de explotación).
- **BAJAS:** 14.563.

Crecimiento Exponencial de Hallazgos por Sector (2024 vs 2025): El aumento en la capacidad de detección se refleja en el comparativo interanual mostrado en la gráfica de líneas:

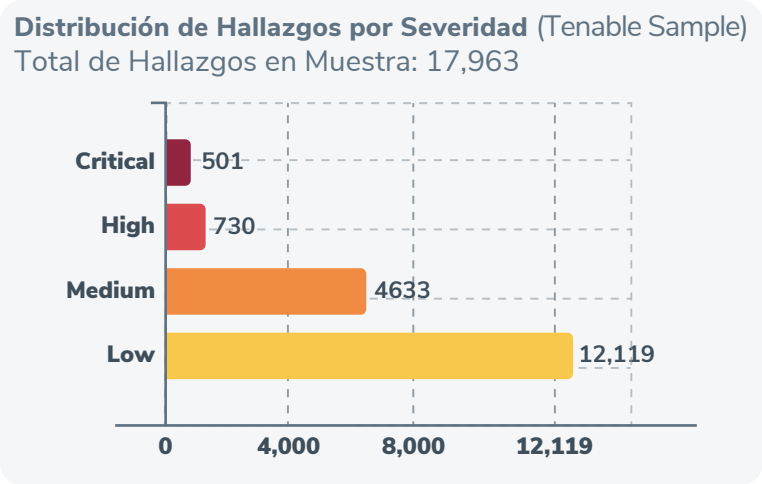


- **Sector Nacional:** Pasamos de detectar 458 hallazgos en 2024 a 10.949 en 2025.
- **Sector Territorial:** Un aumento drástico de 118 a 8.791.
- **Sector Privado:** : De apenas 4 hallazgos visibles en 2024 a 5.760 gestionados en 2025.

Gráfica 3: Tablero de Control 2025: Panorama de Riesgo y Crecimiento. Se evidencia un aumento exponencial en la detección de hallazgos en el último año (de ~580 en 2024 a más de 25.500 en 2025 en los tres sectores), con un total de 74.541 vulnerabilidades identificadas sobre una superficie de 35.424 activos revisados. Los riesgos Críticos y Altos concentran 27.404 vulnerabilidades de atención prioritaria (incluyendo 844 de riesgo inminente). Crecimiento exponencial de hallazgos por sector (2024 vs 2025)

PROFUNDIZACIÓN TÉCNICA: EL DESAFÍO DEL "RUIDO" VS. EL RIESGO REAL

Utilizando herramientas avanzadas como Tenable, el equipo de analistas se enfrenta al reto de filtrar el "ruido" para enfocarse en lo verdaderamente peligroso. La siguiente gráfica, extraída directamente de nuestros análisis técnicos, ilustra la distribución típica de los hallazgos en una muestra representativa en sitios web:



Gráfica 3: Distribución de hallazgos por severidad en Tenable. Muestra cómo el volumen de vulnerabilidades bajas (12.119) puede ocultar las críticas (501) y altas (730).

El análisis de esta gráfica nos muestra que la inmensa mayoría de alertas (más de 12.000 en esta muestra) son de severidad baja. La estrategia de ColCERT en 2025 ha sido no distraerse con el volumen, sino atacar las vulnerabilidades Críticas (501) y Altas (730) mostradas en la gráfica, que son las puertas de entrada para ataques de Ransomware y exfiltración de datos.

Distribución Geográfica del Riesgo y Hallazgos Recurrentes

Gracias a la descentralización, evidenciamos que el riesgo ya no es exclusivo de Bogotá. Si bien la capital concentra una gran parte de los activos (estimado en 8.098), departamentos como Antioquia, Boyacá, Nariño y la región Caribe presentan ahora una infraestructura digital crítica que exigió nuestra intervención directa.

Los 3 Vectores de Ataque (Jerarquizados 2025):

El análisis de profundidad sobre las vulnerabilidades críticas revela un cambio en el patrón de amenaza, destacando la Deuda Técnica como el principal adversario, tal como se visualiza en nuestros tableros de control:

- **Obsolescencia Tecnológica (El Enemigo #1):** Representa el riesgo más crítico. El uso extendido de versiones de PHP y Apache sin soporte (End-of-Life) expone a las entidades a Ejecución Remota de Código (RCE) inmediata.



- **Configuración Deficiente de Correo:** La ausencia de protocolos SPF, DKIM y DMARC sigue siendo la puerta de entrada principal para campañas de phishing y suplantación institucional.
- **Superficie de Ataque Expuesta:** La persistencia de puertos de gestión (SSH, RDP, bases de datos) abiertos innecesariamente a internet facilita ataques de fuerza bruta automatizados.

Conclusión

El balance 2025 de ColCERT demuestra un éxito rotundo en la ampliación de la capacidad de visibilidad y velocidad de respuesta. Hoy Colombia ve más y responde más rápido. El reto para el próximo periodo no es solo detectar, sino acelerar los tiempos de remediación de las vulnerabilidades críticas identificadas y cerrar las brechas recurrentes en la higiene de ciberseguridad nacional.

PROYECCIÓN
DE LAS AMENAZAS



- El entorno geopolítico, las innovaciones tecnológicas y la incidencia de los atacantes presentan una tendencia creciente y sostenida de la complejidad y persistencia de las ciberamenazas. La convergencia entre IA generativa, sistemas industriales conectados y automatizados (OT/ICS) y tensiones geoestratégicas genera nuevos escenarios que pueden incidir en el ecosistema digital de Colombia.
- El escenario más probable para el primer semestre de 2026, es la **intensificación de ciberataques dirigidos contra infraestructuras críticas con el uso de las herramientas de IA generativa, la explotación de vulnerabilidades por fallas en segmentación de la red.**
- Esto especialmente se da mediante **phishing, deepfakes, bypass de MFA y automatización de reconocimiento.** Lo anterior, impacta tanto al sector público, las empresas y las familias, dada la proliferación de vulnerabilidades sin parches ICS/OT y sistemas heredados en Latinoamérica.

PROYECCIÓN DE LAS AMENAZAS

- Esas vulnerabilidades persistentes tienden a incidir sobre los **sectores de salud, educación, energía, agua, transporte y el sector financiero/bancario.** Además, es probable que continue la afectación sobre la administración local y entidades de gobierno.

  Sin embargo, puede existir una repuesta ante las amenazas sí se continúan los avances en ciberresiliencia institucional, que viene de la implementación y **creación de los CERT sectoriales, las alianzas con CISA, FIRST, sector privado y OEA.**

- Además de la adopción de medidas de Zero Trust y la formación y capacitación de talento humano que continue en el tiempo.

Las Amenazas que más se pueden presentar son:

- **Cibercrimen-as-a-Service (CaaS)**
- **Automatización de ataques por IA**
- **Ciberespionaje regional**
- **Ataques a la cadena de suministro**
- **Deepfake y manipulación de información**
- **Criptojacking e infraestructura en nube comprometida**

ESCENARIOS ALTERNATIVOS

› En este espacio se presentan alternativas que pueden generar afectaciones para el Estado, teniendo encuentra el escenario más crítico y de mayor impacto.



- Para el segundo semestre de 2025 y 2026 se presenta un aumento sostenido de ataques Ransomware con doble extorsión sobre la infraestructura crítica cibernética. Este escenario se dirige a Sistemas de Control Industrial (ICS) y afecta servicios públicos **de agua, salud, energía,** aplicando tácticas de cifrado. Lo anterior, evidenciado por tendencias de LATAM como TrendMicro o CrowStrike.

- En Colombia se evidencia un incremento de campañas de suplantación institucional y phishing con IA generativa, a partir de mayor incidencia de hacktivistas y grupos criminales, afectando a entidades de gobierno, con el objetivo de robar datos y manipular la opinión pública. Esto podría ocurrir en contextos de alta actividad política o electoral, lo que podría impactar la percepción pública y la confianza en las instituciones.

- Se mantiene la tendencia de menos reportes formales al ColCERT, no por menos ataques, sino por subregistro, desconexión entre los niveles de gobierno y la tercerización de los servicios de TI. Este escenario afecta a entidades territoriales del orden local, municipios pequeños y servicios descentralizados. Lo anterior, evidencia dificultad para focalizar los recursos y la coordinación de una respuesta por capacidades limitadas.

IMPACTO

TENDENCIA DE AMENAZAS
2025 - 2026

Categoría	Tendencia proyectada	Ejemplo/actor asociado
1. Cibercrimen-as-a-Service (CaaS)	Mayor sofisticación y disponibilidad de kits maliciosos (ransomware, DDoS, phishing con IA)	LockBit 3.0, Black Basta
2. Automatización de ataques por IA	Automatización de ataques, evasión de controles y manipulación de datos	Emulación de usuarios, evasión de EDR
3. Ciberespionaje regional	Enfoque en entidades gubernamentales, diplomáticas y judiciales	APT10, APT34, Turla
4. Ataques a la cadena de suministro	Abuso de proveedores TI nacionales (software, ISP, integradores)	Ataques similares a SolarWinds, MOVEit
5. Deepfake y manipulación informativa	Uso con fines de desinformación electoral o extorsión	Amenaza híbrida con IA y redes sociales
6. Criptojacking e infraestructura en nube comprometida	Explotación de entornos cloud mal configurados y minería oculta	Cloud Hopper, XMRig-based botnets
7. Ataques centrados en la identidad en nube/SaaS	Mayor explotación de proveedores de identidad y expansión hacia identidades no humanas como agentes de IA.	APT 29/ comprometió identidades en la nube al evadir MFA, inyectando aplicaciones OAuth maliciosas en entornos corporativos

Análisis

- Las ciberamenazas en Colombia y la región se enmarcan en la convergencia del creciente uso de la IA, la baja higiene digital y el creciente número de estructuras criminales híbridas.

  Los ataques dirigidos al sector salud, empresas de energía y operadores o terceros asociados a entidades públicas de gobierno vía cadenas de suministro tienden a ser los más críticos.

- Es probable que los patrones de ataque de las APT migren a operaciones más sigilosas o se proyecten hacia objetivos a largo plazo. En ese sentido, las botnets pueden resurgir como herramientas económicas y escalables para campañas de cibercrimen y ataques híbridos, incluidas campañas masivas de denegación de servicio (DDoS), distribución de malware y explotación de IoT.

Sector	Vectores más frecuentes	Tendencias clave 2025-2026
Infraestructura crítica	Ransomware, DDoS, ICS exploits	Ciberresiliencia nacional, cooperación internacional
Salud	Ransomware, phishing, IoMT exploits	Extorsión económica y disrupción funcional
Finanzas	DDoS, phishing, acceso web, ransomware	Campañas motivadas por tensiones geopolíticas y dinero
Educación	Ransomware, phishing, acceso a LMS	Exposición alta por digitalización acelerada
Espacio	Supply chain, jamming, malware firmware	Nueva frontera de ciberdefensa
Manufactura	IoT/OT malware, firmware, red mal segmentada	Foco en industria 4.0 y automatización
Gobierno/Defensa	APT, espionaje, ransomware político	Ciberespionaje estatal, ciberwarfare y hacktivismo

Recomendaciones estratégicas

- **Implementar un marco de detección nacional proactivo**, articulado con sectores críticos (Zero Trust + monitoreo continuo + IA).
- Implementación de básicos de seguridad del modelo MSPI del ministerio TIC y estándares internacionales como la ISO-27001.
- **Adoptar un proceso de generación de confianza con actores públicos y privados** que se apoye en el reporte de incidentes cibernéticos críticos.
- **Desarrollar una capacidad nacional para pruebas de seguridad por diseño.**
- **Fomentar entornos controlados para IA defensiva (Red-Blue-Purple Teams con IA generativa).**





- **Creación de los CERT sectoriales, esto va de la mano con una red interoperable**, priorizando sectores de energía, educación, salud y agua.
- **Alinear incentivos fiscales con adopción de controles NIST SP 800-53 o ISO 27001 para PYMEs.**
- Protección avanzada de identidades y accesos, con autenticación **multifactor** resistente y monitoreo en tiempo real basado en IA para detectar anomalías.
- **Capacitación continua y reforzamiento en seguridad de IoT, endpoints y aplicaciones para mitigar vectores de ataque con ingeniería social, phishing avanzado y explotación zero-day.**

Resumen de las fuentes y nivel de confianza en la información proporcionada

El presente análisis se basa en el uso de fuentes abiertas, estadísticas del ColCERT, y el uso de documentos oficiales de entidades como CISA, CCN-CERT, entre otros, aunque existe un limitante en la información disponible reportada, se recoge información de tanques de pensamiento, medios de comunicación, actores estatales, entre otros. En todos los casos se contrastan las fuentes diversas y actualizadas, medios especializados y fuentes oficiales disponibles. La confianza en la información es alta, aunque se reconoce que las ciber amenazas evolucionan de forma constante, por lo que existe un margen de incertidumbre en las proyecciones y análisis presentados de lo que se espera en el próximo año.

1. CrodStrike, 2025, Informe sobre el panorama de amenazas en América Latina para el 2025, https://www.crowdstrike.com/es-latam/resources/reports/crowdstrike-2025-latin-america-threat-landscape-report/

2. CISA. (2025). 2024 Year in Review. U.S. Department of Homeland Security. Recuperado de https://www.cisa.gov/sites/default/files/2024-02/CISA-Year-in-Review-2024.pdf

3. CISA, 2025, Known Exploited Vulnerabilities Catalog, https://www.cisa.gov/known-exploited-vulnerabilities-catalog?page=8

4. CISA. (2025). Cybersecurity Performance Goals Adoption Report. Recuperado de https://www.cisa.gov/sites/default/files/2025-01/CPG-Adoption-Report-Jan2025.pdf

5. CISA. (2025). FY 2025–2026 International Strategic Plan. Recuperado de https://www.cisa.gov/sites/default/files/2025-04/cisa-international-strategic-plan-2025-2026.pdf

6. NIST. (2025, abril 3). SP 800-61 Revision 3: Computer Security Incident Handling Guide. Recuperado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/-NIST.SP.800-61r3.pdf

7. ENISA. (2025, marzo 26). Space Threat Landscape 2025. Recuperado de https://www.enisa.europa.eu/publications/space-threat-landscape-2025

ANEXO 1. ATAQUES RECIENTES CON MAYOR IMPACTO

	Entidad	Fecha	Tipo de ataque	Impacto / Detalles	Fuentes
1	Justicia Penal Militar y Superintendencia de la Economía Solidaria	15-jun-25	Malware / interrupción	Suspensión de términos judiciales; sistemas en nube y redes comprometidos	https://www.infobae.com/colombia/2025/06/17/ciberataque-a-la-justicia-penal-militar-obligo-a-suspender-terminos-judiciales-y-atencion-tecnologica/
2	Empresas Municipales de Cali (Emcali)	13-may-25	Ciberataque IT (Posible ransomware)	No identificado	https://www.emcali.com.co/w/por-posible-ataque-informatico-al-sistema-de-emcali-se-encuentran-temporalmente-suspendidos-algunos-servicios-de-informacion
3	Autoridad Nacional de Acuicultura y Pesca (AUNAP)	13-may-25	Ataque al sitio web (DDOS / defacement)	No identificado	Comunicado oficial
4	IFX Networks (afectó 30+ entidades)	12-sept-2024	Ransomware	Afectó Ministerio de Salud, SIC, Rama Judicial, ICA, etc.	https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/278831:Gobierno-Nacional-atiende-ataque-cibernetico-que-afecta-a-varias-entidades-e-instala-PMU-CIBER
5	Air-e (operador privado que distribuye y comercializa energía eléctrica en Atlántico, Magdalena y La Guajira)	6-sep-24	Incidente informático / posible ransomware	Interrupción de facturación; datos potencialmente comprometidos de 2.3M usuarios	https://elpais.com/america-colombia/2024-10-24/el-ciberataque-contra-air-e-planta-un-nuevo-obstaculo-para-el-rescate-de-la-energetica-responsable-de-media-region-caribe.html?utm_source=chatgpt.com
6	Hospital Universitario de Caldas	20-mar-24	Ransomware	Cibercriminal (no confirmado)	Comunicado oficial

ANEXO 2. APT MÁS RELEVANTES EN AMÉRICA LATINA

Desconocido

APT-C-43 (Machete)
Motivación: Espionaje militar y gubernamental
Afecta: Venezuela, Ecuador, Colombia, Nicaragua.

Colombia

APT-C-36 (Blind Eagle)
Motivación: Ciberespionaje y fraude Afecta: Colombia, Ecuador, Perú, Chile.

Irán

APT39
Motivación: Espionaje y monitoreo
Afecta: Venezuela, Brasil.

APT35 (Charming Kitten)
Motivación: ciberespionaje y desinformación
Afecta: Argentina, Venezuela.

APT34 (OilRig)
Motivación: Espionaje y sabotaje
Afecta: Brasil, México.

APT33
Motivación: Espionaje y ciberataques
Afecta: México, Colombia.

China

APT41
Motivación: Espionaje y cibercrimen
Afecta: Brasil, Chile, México.

APT40
Motivación: Robo de propiedad intelectual
Afecta: Brasil, Argentina, México.

APT10
Motivación: Robo de datos y espionaje
Afecta: Brasil, Chile, Perú.

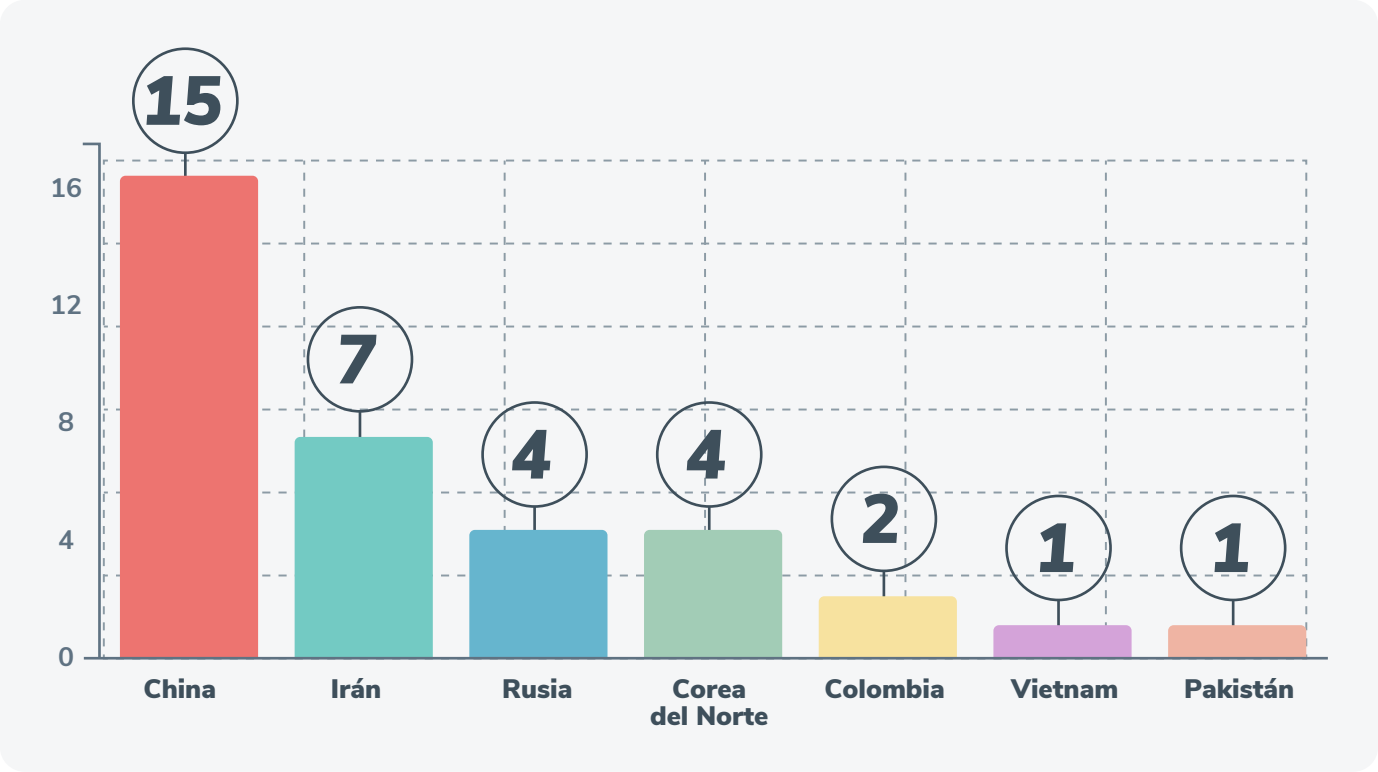
Rusia

APT29 (Cozy Bear)
Motivación: Espionaje político y económico
Afecta: Brasil, México, Venezuela.

APT28 (Fancy Bear)
Motivación: Ciberespionaje y desinformación
Afecta: Brasil, Argentina.

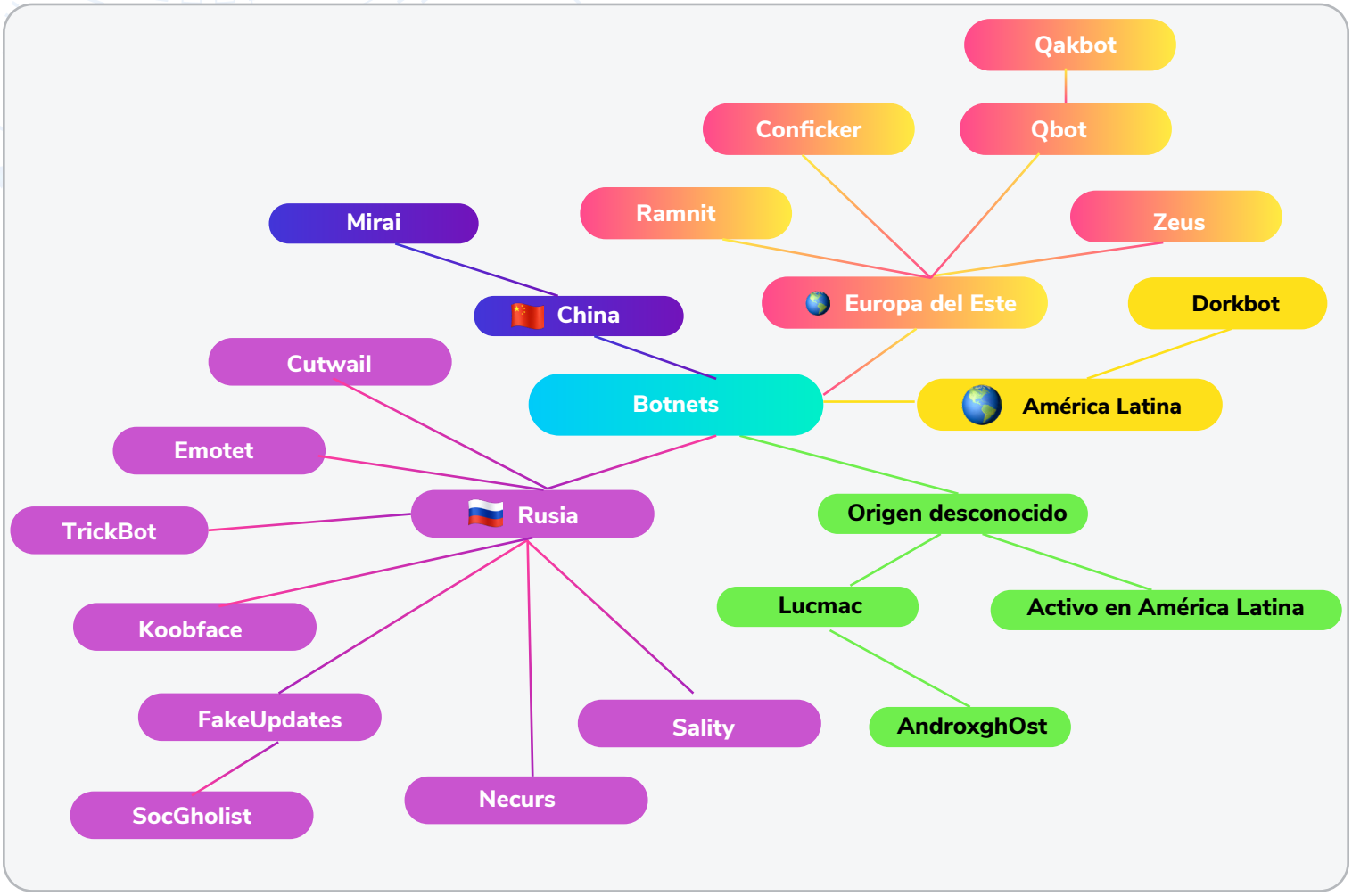
ANEXO 3. APT POR PAÍS

NÚMERO DE GRUPOS
APT POR PAÍS

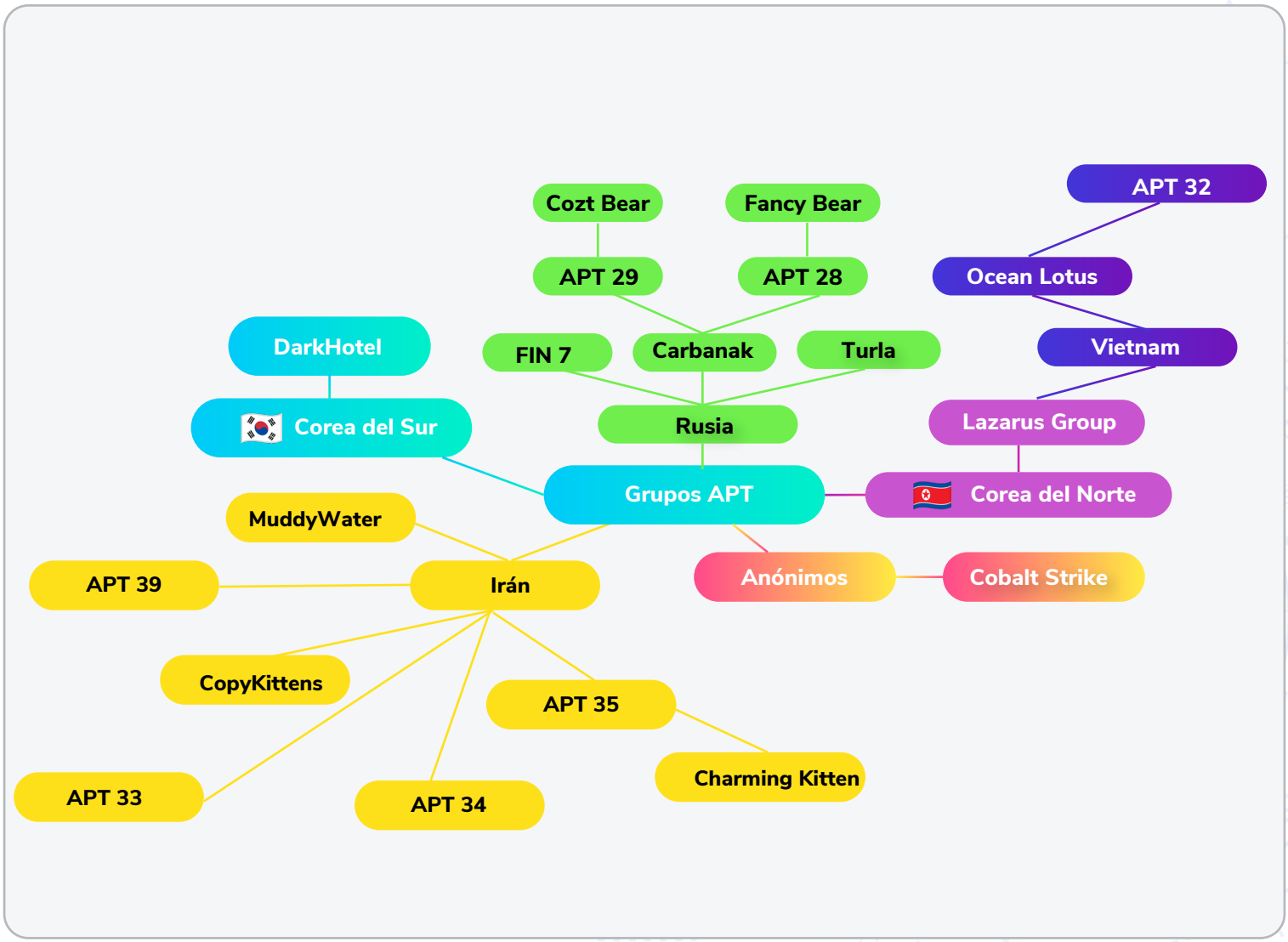


ANEXO 3. AMENAZAS MÁS RELEVANTES 2024 - 2025

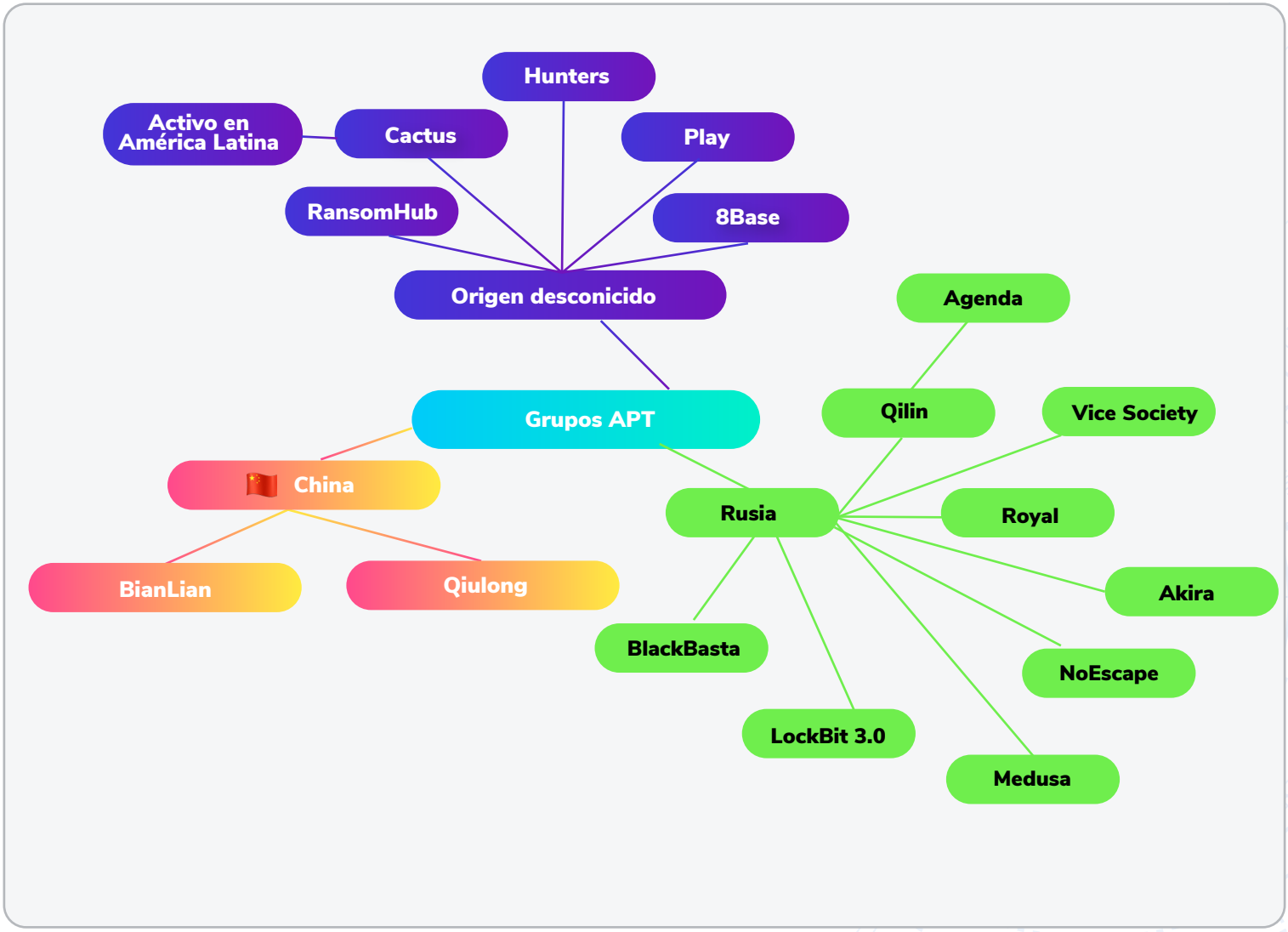
BOTNET



APT


APT 32
Cozt Bear
Fancy Bear
APT 29
APT 28
Ocean Lotus
DarkHotel
FIN 7
Carbanak
Turla
Vietnam
Corea del Sur
Rusia
Lazarus Group
Grupos APT
Corea del Norte
MuddyWater
APT 39
Irán
Anónimos
Cobalt Strike
CopyKittens
APT 35
Charming Kitten
APT 33
APT 34

RANSOMWARE


Hunters
Activo en América Latina
Cactus
Play
RansomHub
8Base
Origen desconicido
Agenda
Grupos APT
Qilin
Vice Society
China
Rusia
Royal
BianLian
Qiulong
Akira
BlackBasta
NoEscape
LockBit 3.0
Medusa

ANEXO 5. INCIDENTES GESTIONADOS POR EL COLCERT 2025

Durante el año 2025, el equipo **ColCERT** gestionó seiscientos setenta y un (697) incidentes de seguridad digital, reportados por entidades públicas y privadas del país, teniendo en cuenta lo establecido en **la resolución 500 del 2021 del MinTIC,** como se muestra en la siguiente tabla:

Orden de la Entidad	Cantidad Incidentes
Territorial	341
Nacional	117
Privada	239
Total	697

Tabla 1 Número de incidentes gestionados por ColCERT. Elaboración propia

Dentro de las categorías de los incidentes presentados se encuentran los siguientes tipos:

Clase de Incidente	Incidentes 2024	Incidentes 2025	Total	% del Total
Fraude	1,222	475	1,697	87.29%
Intrusión	91	89	180	9.26%
Vulnerable	69	45	114	5.86%
Compromiso de Información	17	59	76	4.42%
Contenido Dañino	14	26	40	2.06%
Disponibilidad	3	3	6	0.31%
Contenido Abusivo	5	0	5	0.26%
Intento de Intrusión	4	0	4	0.21%
Obtención de Información	1	0	1	0.05%

Tabla 2. Categorías de los incidentes gestionados. Elaboración propia

En 2025 se reportaron 671 incidentes, lo que representa una disminución del 46.2% en la cantidad de incidentes reportados. Agosto de 2025 fue el mes con mayor número de incidentes (115), lo que representa un 17.14% del total presentado en el año, hasta cierre del mes de noviembre.

Los meses de julio, agosto y septiembre muestran un patrón consistente en el incremento y reporte de incidentes, lo que evidencia **afectaciones considerables** para entidades gubernamentales y organizaciones privadas en este trimestre.

Mes	2024	2025
Enero	6	39
Febrero	73	34
Marzo	73	35
Abril	104	27
Mayo	130	44
Junio	142	32
Julio	155	94
Agosto	228	115
Septiembre	163	114
Octubre	169	63
Noviembre	96	74
Diciembre	88	26

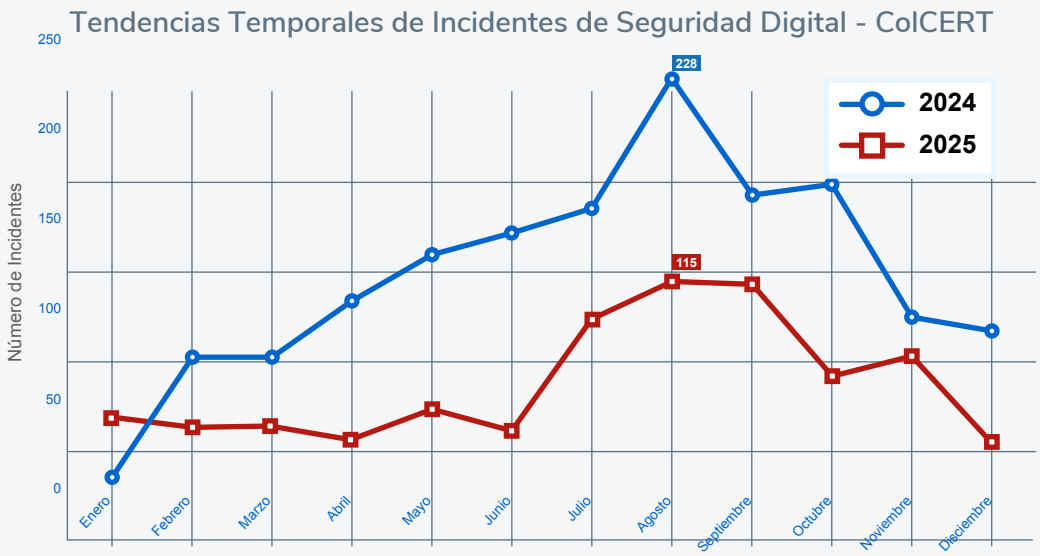


Tabla 3. Tendencia mensual de incidentes (2024 vs.2025). Elaboración propia.

El **fraude** es la clase más común de afectación, representando el **79.83%** de los incidentes totales de los dos últimos años, principalmente por **phishing,** seguido del uso no autorizado de recursos (compromiso de correos electrónicos).

Top 5 Tipos de Incidentes

Tipo de Incidente	Incidentes 2024	Incidentes 2025	Total
Phishing	610	225	835
Uso no autorizado de recursos	534	250	784
Compromiso de aplicaciones (Defacement)	68	69	137
Sistema Vulnerable	26	44	70
Modificación no autorizada de información	7	43	50

Tabla 2: Tipos de Incidentes (2024-2025).

Bogotá D.C. es la región con mayor número de incidentes presentados. Las entidades territoriales son las más afectadas a nivel nacional, lo que sugiere que presentan mayores vulnerabilidades.

Distribución de Incidentes por Región (Top 10)

Departamento	Incidentes 2024	Incidentes 2025
Bogotá D.C	862	363
Antioquia	100	41
Cundinamarca	47	21
Boyacá	34	21
Tolima	32	15
Nariño	31	21
Santander	28	28
Valle del Cauca	26	26
Huila	26	12
Norte de Santander	20	13

Tabla 06. Regiones más afectadas 2024 - 2025. Elaboración propia.

TIC

COLCERT

2025

@colCERT

www.colcert.gov.co