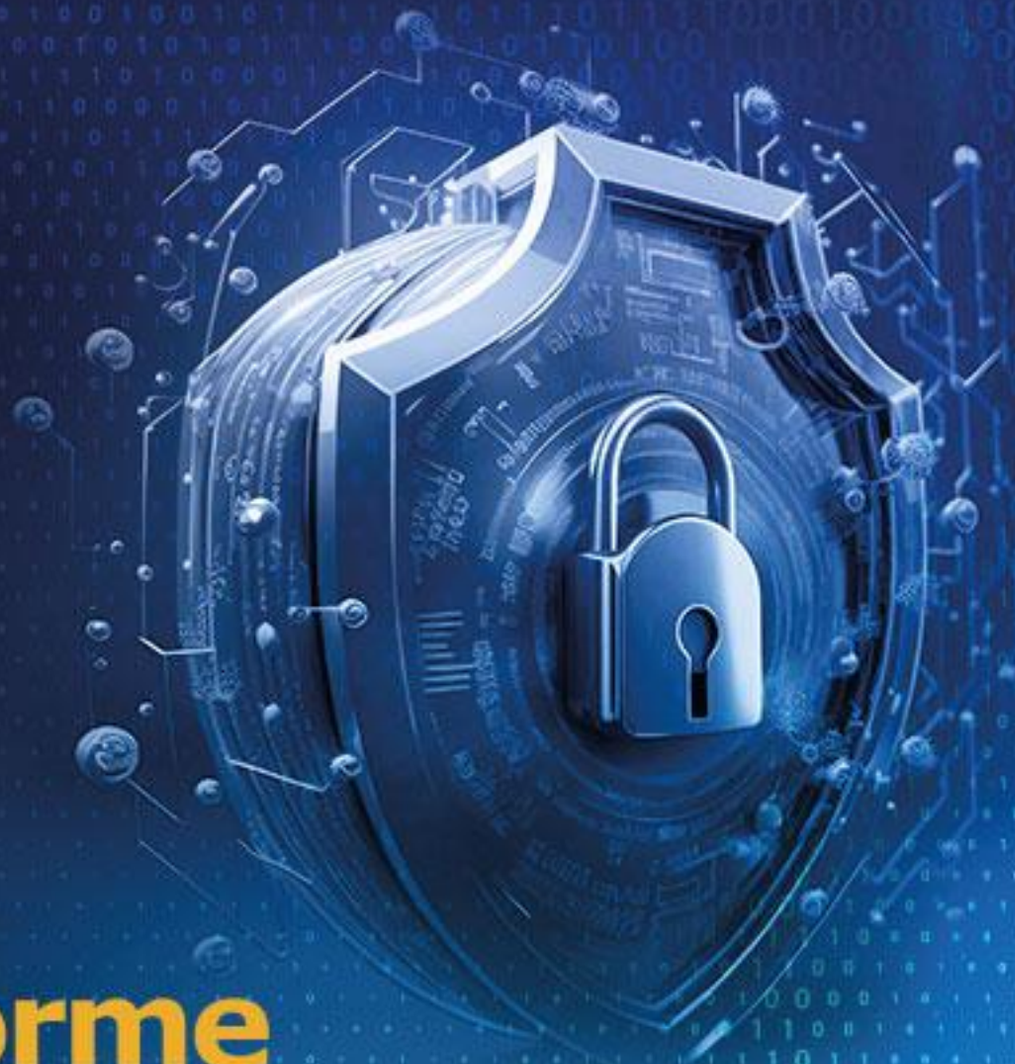
TIC



Informe de campaña

de exfiltración de información

Período analizado: enero – marzo 2026

Metodología: OSINT

IN-20260325-029

COLCERT

Informe

Campaña de exfiltración de Información

Período analizado: enero – marzo 2026 Metodología: OSINT

IN-20260325-029

TIC

TLP: AMBER

Contenido

Resumen Ejecutivo

El presente informe consolida los resultados de un análisis técnico basado en reconocimiento pasivo de fuentes abiertas (OSINT) realizado sobre dominios gubernamentales colombianos. Los hallazgos aquí documentados no constituyen una proyección de riesgo ni un escenario hipotético, sino que describen una situación real ocurrida durante el período comprendido entre enero y marzo de 2026, sustentada en evidencia verificable de explotación activa de datos de ciudadanos colombianos, los cuales ya se encontraban comprometidos y en circulación en mercados clandestinos.

Entre el 9 de enero y el 24 de marzo de 2026, se identificó la actuación de nueve actores maliciosos distintos, quienes comprometieron más de 40 entidades colombianas, pertenecientes a ocho sectores estratégicos. Las actividades observadas no involucraron herramientas de alto costo ni capacidades avanzadas de inteligencia, los atacantes operaron principalmente mediante scripts en Python y módulos de Metasploit de libre acceso. En el caso más crítico de la campaña, la exfiltración de información se produjo a partir del acceso directo a una URL pública sin mecanismos de protección, lo que evidencia fallas básicas de control y exposición prolongada de datos.

Tabla - Distribución de incidentes por sector

Sector	Alcance	CVEs / Vectores	Registros expuestos
Educación superior	11 instituciones	CVE-2024-43425 (RCE Moodle)	>75.000 registros
Salud	>5 entidades	CVE-2021-44228 (Log4Shell), CVE-2025-24799 (GLPI RCE), CVE-2023-23752 (Joomla)	>250.000 registros de pacientes
Gobierno nacional	7 entidades	CWE-306 (API sin autenticación), Apache 2.2.x EOL	18M registros (estimado — sistema de agendamiento ciudadano)
Gobierno territorial	5 entidades	Proveedor TI compartido (punto de falla único)	No cuantificado
Sector financiero	3 entidades	Credenciales reutilizadas	En proceso de verificación
Transporte / Logística	2 entidades	Sistemas legacy EOL	661.126 registros

El denominador común identificado en los incidentes analizados es la ausencia de un proceso funcional de gestión de vulnerabilidades. Al momento del compromiso, el 96 % de las entidades evaluadas presentaba una postura de seguridad desatendida, caracterizada por exposiciones conocidas, controles básicos inexistentes o sin mantenimiento, y ausencia de mecanismos sistemáticos de detección y remediación.

CASO EMBLEMÁTICO - DATOS DE LOS AFILIADOS AL SGSSS EXPUESTOS: Una instancia de SharePoint Server 2013 (fin de soporte: abril 2023) en un portal del sector salud expone el endpoint /_api/Web/Lists/Items(N) sin ninguna autenticación. La API retorna nombre completo, número de cédula y EPS del afiliado al SGSSS colombiano. No se requiere exploit ni conocimiento especializado: unas líneas de Python son suficientes para consultar cualquier registro

2. El Estado de la Infraestructura Digital: Un problema estructural

Los hallazgos indican que Colombia no ha sido afectada, en este período, por actores con capacidades avanzadas de inteligencia o herramientas sofisticadas. Los compromisos observados corresponden a actores oportunistas que emplearon herramientas de uso gratuito y técnicas ampliamente conocidas, aprovechando una superficie de ataque expuesta a Internet, con brechas de seguridad continuas y ausencia de capacidades de detección y monitoreo en las entidades comprometidas.

2.1 Exposición reconocible en minutos a través de reconocimiento pasivo de fuentes abiertas

El reconocimiento pasivo constituye la fase inicial de observación previa a cualquier intrusión, y se limita a la consulta de fuentes públicas, accesibles y legalmente disponibles. A partir de este tipo de análisis, las fuentes abiertas examinadas revelaron la siguiente información sobre la infraestructura digital colombiana:

- Versión exacta de Moodle, consultando el archivo /lib/upgrade.txt o los encabezados de respuesta HTTP. Con la versión exacta y la base de datos NVD, el atacante sabe en segundos si hay un módulo de Metasploit disponible.
- Lista completa de subdominios activos de cada dominio gov.co y edu.co, incluyendo entornos de staging, APIs internas y paneles de administración no intencionalmente públicos, consultando crt.sh sin ninguna autenticación.
- Versiones exactas de Apache, IIS, PHP y OpenSSL en producción, visibles en los encabezados de respuesta HTTP. X-Powered-By: PHP/7.4 le indica al atacante exactamente qué CVEs aprobechar.
- Ausencia universal de HSTS, CSP, X-Frame-Options y X-Content-Type-Options: una característica compartida por el 100% de los dominios analizados, que refleja que la seguridad no fue considerada en el diseño ni en el despliegue de esos sistemas.

Nota analítica: La información requerida para que un actor malicioso planifique una acción contra una entidad se encuentra, en gran medida, disponible en fuentes públicas y no es posible eliminarla por completo. La cuestión relevante no es la existencia de dicha información, sino si, al momento de su eventual utilización, la entidad contará con controles efectivos que limiten su aprovechamiento, o si persistirán las mismas condiciones de exposición que ya fueron observadas de manera recurrente en múltiples entidades del país.

2.2 La brecha estructural entre exposición y protección

NyxarGroup, identificado como el actor con mayor actividad durante la campaña, creó su perfil en foros clandestinos en febrero de 2026. En un período inferior a cuatro semanas, logró comprometer 26 entidades colombianas utilizando herramientas de libre acceso y un nivel de conocimiento técnico intermedio. La rápida sucesión de compromisos generó escepticismo entre los propios participantes del foro, quienes cuestionaron inicialmente la autenticidad de las publicaciones debido a que el actor carecía de una reputación previamente consolidada. No obstante, la evidencia recopilada confirmó que dichas capacidades fueron suficientes para materializar los compromisos observados.

Factor	El atacante	La entidad
Tiempo requerido	Días para comprometer 26 entidades	Meses sin implementar controles básicos
Inversión económica	Cero: herramientas gratuitas	Recursos presupuestales disponibles sin asignar
Conocimiento técnico	Básico: Metasploit, Python	No requerido para defensas básicas (MFA, parches)
Herramientas utilizadas	Metasploit, scripts automatizados	Ninguna SIEM, WAF ni EDR documentada
Riesgo asumido	Bajo	Alto: datos de millones de ciudadanos expuestos

3. Análisis de Hallazgos por Sector

3.1 Sector Educativo: el más afectado por volumen y velocidad

Once instituciones educativas fueron comprometidas en un lapso de cinco días. La concentración de eventos entre el 22 y el 26 de febrero de 2026 no responde a un comportamiento aleatorio, sino que corresponde a la ejecución sistemática de una metodología automatizada. Un mismo script fue desplegado contra múltiples objetivos que compartían una vulnerabilidad común (CVE 2024 43425 en Moodle), generando compromisos a escala en un período inferior a una semana. El parche de seguridad correspondiente había sido publicado en agosto de 2024; sin embargo, para el momento de los incidentes, las instituciones afectadas aún no lo habían aplicado, acumulando un retraso superior a seis meses.

Las instituciones educativas gestionan y custodian activos de información de alto valor, entre ellos datos de identificación personal, historiales académicos completos, resultados de investigación, propiedad intelectual, credenciales de acceso a redes académicas internacionales y datos asociados a empleabilidad. Una vez exfiltrada, este tipo de información no es recuperable, lo que amplifica de manera significativa el impacto operativo, reputacional y estratégico de los compromisos observados.

3.2 Sector Salud: el riesgo sobre la continuidad asistencial

El sector salud concentra uno de los escenarios de mayor criticidad, al combinar vulnerabilidades técnicas de alto impacto en sistemas que procesan información altamente sensible, con consecuencias potenciales directas sobre la continuidad de los servicios clínicos. Un incidente de ransomware exitoso contra una institución hospitalaria no se limita a la afectación o pérdida de datos; puede derivar en la interrupción de procesos asistenciales críticos, con impacto inmediato sobre la atención de los pacientes y, en determinados contextos, sobre su integridad y seguridad.

- Aplicaciones clínicas sin autenticación: acceso libre a historias clínicas, atención pre-hospitalaria, planificación familiar, radiología, ecografías, epidemiología y facturación.
- Clave API de producción en HTML público (Base64): una clave con acceso completo al sistema de PQRS de una entidad de salud estaba codificada en Base64 en el código HTML público. Base64 no es cifrado: se decodifica en milisegundos.
- Log4Shell cuatro años sin parchar: CVE-2021-44228 (CVSS 10.0), publicado en diciembre de 2021, presente con alta probabilidad en sistemas de historias clínicas basados en Java.
- Divulgación con presión extorsiva: un actor publicó documentos PDF con resultados de laboratorio clínico, incluyendo diagnósticos oncológicos y pruebas genéticas.

3.3 Gobierno: Dependencia crítica de proveedores externos

Los incidentes identificados en entidades gubernamentales presentan el mayor impacto potencial, dado el volumen de ciudadanos directamente afectados. El caso de mayor criticidad corresponde al compromiso de un sistema de agendamiento institucional utilizado por millones de colombianos para la realización de trámites oficiales. El acceso no autorizado se originó en una vulnerabilidad previamente conocida en la plataforma del proveedor externo responsable de su desarrollo y operación, la cual no había sido corregida mediante la aplicación del parche correspondiente al momento del compromiso

4. Inventario de vulnerabilidades críticas identificadas

El siguiente inventario fue elaborado a partir de análisis pasivo de fuentes públicas y abiertamente accesibles. Cada CVE y CWE referenciado cuenta con respaldo verificable en las bases de datos oficiales del NIST. Para la obtención de esta información no se realizó acceso no autorizado ni interacción directa con los sistemas analizados.

CVE / CWE	CVSS	Severidad	Descripción	Sector
CVE-2024-43425	9.8	CRÍTICO	RCE en Moodle 4.x. Módulo Metasploit disponible. Parche disponible desde agosto 2024.	Educación
CVE-2021-44228	10.0	CRÍTICO	Log4Shell. Sistemas de historia clínica en Java expuestos más de 4 años después del parche.	Salud
CVE-2023-23752	7.5	CRÍTICO	Filtración de credenciales MySQL en Joomla vía GET. En CISA KEV. Sin parche aplicado en 2026.	Salud
CVE-2025-24799	9.6	CRÍTICO	SQLi con RCE sin autenticación en GLPI. Expone historia clínica completa.	Salud
CVE-2022-26352	9.8	CRÍTICO	RCE pre-autenticado en dotCMS.	Salud
CVE-2017-7679 + Apache 2.2.x	9.8	CRÍTICO	Buffer overflow en Apache EOL (2017). Versión 2.2.25 en producción en 2026. Sin solución.	Gobierno
CVE-2018-12613 (phpMyAdmin)	8.8	ALTO	LFI escalable a RCE. phpMyAdmin expuesto con PHP vulnerable en plataforma de formación.	Educación
CWE-306	N/A	CRÍTICO	API SharePoint 2013 EOL sin autenticación. Retorna nombre, cédula y EPS de afiliados al SGSSS.	Salud

Observación crítica: Todas las vulnerabilidades identificadas contaban con parches disponibles con anterioridad a la ocurrencia de los compromisos. En el caso de CVE 2024 43425, el parche había sido publicado en agosto de 2024; Log4Shell, desde diciembre de 2021; y CVE 2023 23752, desde enero de 2023. Los eventos observados no se explican por la ausencia de soluciones técnicas, sino por la inexistencia de un proceso sistemático que permita identificar software vulnerable, evaluar y priorizar el riesgo asociado, y aplicar los parches dentro de plazos razonables. Este conjunto de prácticas corresponde a lo que se conoce como Gestión de Vulnerabilidades (Vulnerability Management Process – VMP).

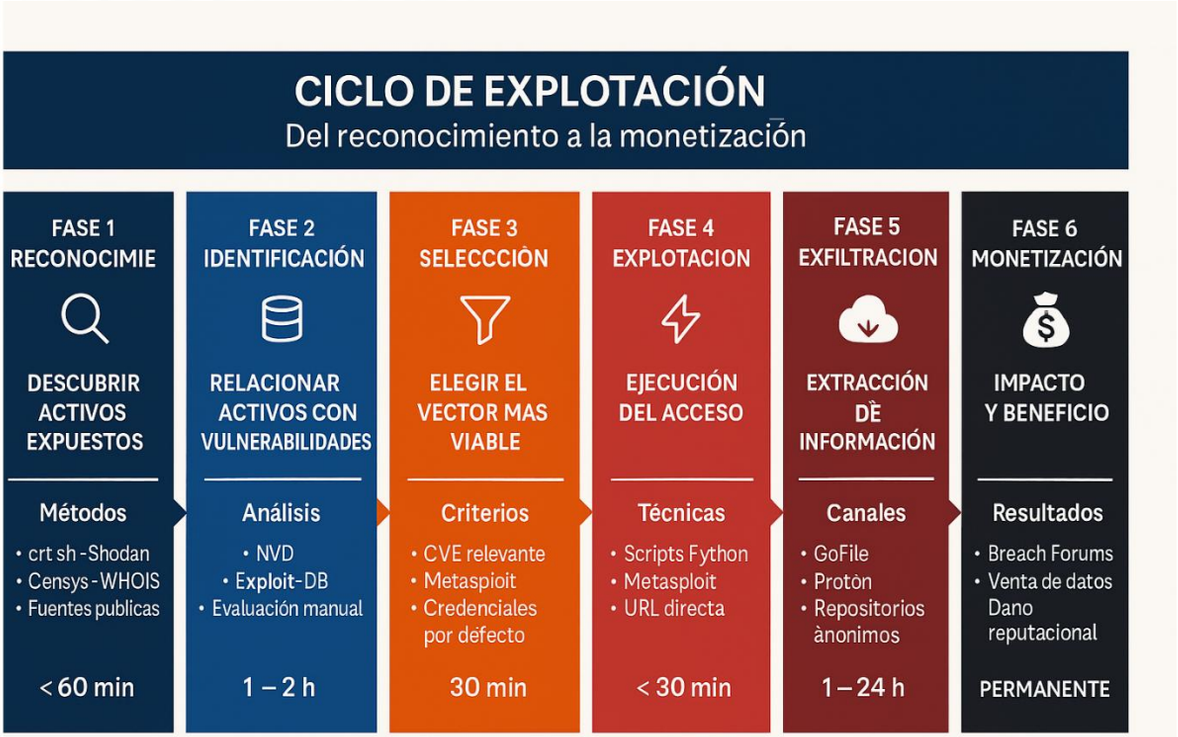
5. Obsolescencia Tecnológica: Plataformas sin soporte que amplifican el riesgo

El software que ha alcanzado su estado de fin de vida (End of Life, EOL) constituye una categoría de riesgo particularmente crítica, en este contexto, cada nueva vulnerabilidad identificada permanece expuesta de forma indefinida, al no existir parches o actualizaciones de seguridad disponibles por parte del fabricante, la única medida de mitigación viable es la migración a plataformas soportadas. En ausencia de esta transición, el riesgo asociado no se reduce ni se estabiliza, sino que se incrementa progresivamente en el tiempo.

Software EOL	Fin de soporte	Sector	Riesgo activo
SharePoint Server 2013	Abril 2023	Salud	API expone datos de afiliados al SGSSS sin autenticación.
PHP 5.6.x	Dic 2018 (+7 años)	Educación	CVE-2019-11041/42. Vulnerabilidades heap sin posibilidad de parche.
Apache 2.2.x	Jul 2017 (+9 años)	Gobierno	CVE-2017-7679 CVSS 9.8. Versión 2.2.25 en producción. Sin solución.
Moodle 3.8.4	Mayo 2021 (+5 años)	Educación	SQLi y escalada de privilegios activos. Miles de registros expuestos.
OpenSSL 1.0.2l	Dic 2019 (+7 años)	Gobierno	DROWN, CVE-2016-0800. TLS 1.0 /1.1 habilitados. Permite descifrado de tráfico.
Java / Log4j < 2.17.1	Dic 2021 (+4 años)	Salud	CVE-2021-44228 CVSS 10.0. Sistemas que continúan expuestos.

6. Flujo Visual: Secuencia de actuación de un actor malicioso

El siguiente flujo representa las seis fases del ciclo de explotación identificadas en los incidentes analizados, mapeadas con referencia al marco MITRE ATT&CK. Los tiempos asociados a cada fase corresponden a intervalos observados o estimados a partir de la evidencia recopilada durante la campaña registrada entre enero y marzo de 2026.



Fuente: Construcción Propia

Contexto: NyxarGroup comprometió 26 entidades en un período inferior a cuatro semanas, empleando herramientas de libre acceso y un nivel de conocimiento técnico intermedio, con un costo operativo prácticamente nulo para el atacante. De forma paralela, las medidas que habrían permitido prevenir aproximadamente el 80 % de los compromisos observados no implicaban inversiones significativas; actualización de plataformas como Moodle (software gratuito), eliminación de credenciales predeterminadas (sin costos de licenciamiento) y restricción de acceso a interfaces administrativas mediante configuraciones básicas. La diferencia crítica entre el éxito del ataque y la eficacia de la defensa no fue de carácter presupuestal, sino de decisión organizacional y existencia de procesos operativos mínimos.

7. Fallas de Configuración Sistémicas

Más allá de la presencia de versiones de software vulnerable, el análisis evidenció fallas recurrentes de configuración que incrementan la superficie de ataque de manera independiente del estado de parcheo. Estas condiciones derivan de prácticas inadecuadas en el diseño, despliegue y operación de los sistemas, y en numerosos casos pueden ser corregidas mediante ajustes básicos, con costos de implementación bajos o inexistentes.

Falla de configuración	Prevalencia	Costo corrección	Riesgo
Paneles /admin/ accesibles desde internet	Instancias Moodle	Bajo	Fuerza bruta automatizada desde cualquier IP.
Cabeceras HTTP de seguridad ausentes	Dominios analizados	Bajo	XSS, clickjacking, MIME-sniffing sin control.
Versiones de software expuestas en headers	>90% servidores	Bajo	X-Powered-By: PHP/7.4 → el atacante sabe qué CVE usar.
APIs REST sin rate limiting	Instancias Moodle	Bajo	Enumeración masiva de usuarios en segundos.
HSTS no implementado	Dominios analizados	Bajo	Permite downgrade a HTTP. Tráfico capturable.
Cookies sin HttpOnly/ Secure	Sectores afectados	Bajo	Robo de sesión vía XSS. Acceso total como usuario activo.
MFA no obligatorio para administradores	Generalizado	Bajo	Credencial comprometida = acceso total sin segundo factor.
Subdominios expuestos en certificado SAN	Dominios analizados	Bajo	Mapa completo de infraestructura: staging, APIs, admin.

La recurrencia del 100 % en determinadas categorías constituye una evidencia concluyente de que estas condiciones no corresponden a errores aislados o circunstanciales. Los hallazgos reflejan que la seguridad no ha sido integrada de manera sistemática en los procesos de desarrollo, despliegue y operación de los sistemas, y que no se realizan evaluaciones periódicas de la postura de seguridad, lo que permite que estas exposiciones persistan en el tiempo.

8. La cadena de suministro como vector crítico

Cuando una entidad externaliza el desarrollo y el mantenimiento de un sistema crítico a un proveedor tercero, su superficie de ataque se amplía y se extiende hacia la infraestructura y los procesos del proveedor, generalmente sin visibilidad ni control directo por parte de la entidad contratante. En este escenario, el proveedor suele asumir que la seguridad en entornos productivos es responsabilidad del cliente, mientras que la entidad asume que el proveedor gestiona adecuadamente la seguridad del sistema que diseñó y mantiene. El resultado operativo de esta ambigüedad es un vacío de responsabilidad en el que ninguna de las partes ejerce una gestión efectiva de la seguridad.

El patrón identificado cinco entidades comprometidas en un mismo día, constituye un indicador inequívoco de riesgo de cadena de suministro: la dependencia de un proveedor tecnológico común con un punto único de falla, que no fue auditado ni supervisado por las entidades usuarias. Cuando dicho proveedor presenta una falla de seguridad, el impacto se propaga de forma simultánea a todas las organizaciones que dependen de él, multiplicando el alcance y la severidad del compromiso.

Recomendación contractual: Todo contrato asociado al desarrollo, operación o mantenimiento de sistemas institucionales debería incorporar, como mínimo, los siguientes componentes de seguridad:

(1) Una cláusula formal de gestión de vulnerabilidades, con acuerdos de nivel de servicio (SLA) claramente definidos para el parcheo (crítico: 24–72 horas; alto: 7 días; medio: 30 días);

(2) La obligación de notificar incidentes de seguridad en un plazo máximo de 24 horas desde su detección;

(3) El derecho de la entidad a realizar auditorías de seguridad, al menos con periodicidad anual;

(4) La definición explícita de responsabilidades contractuales frente a brechas derivadas de negligencia en la aplicación de parches o controles acordados; y

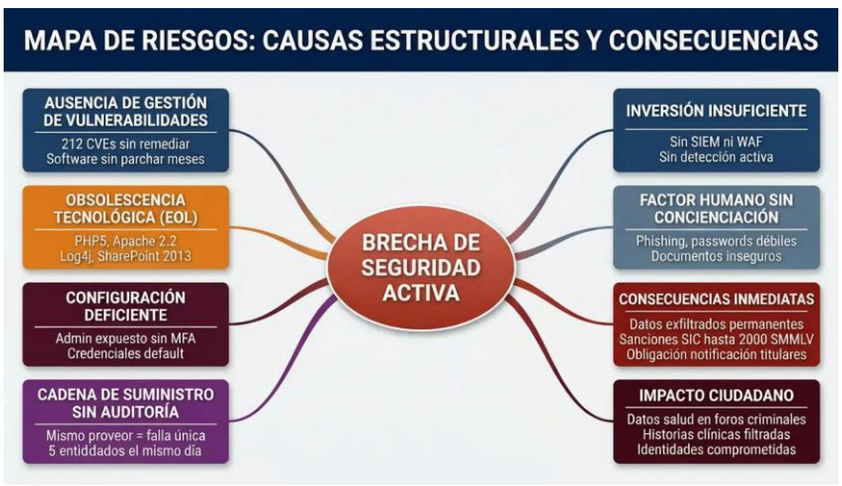
(5) La prohibición expresa del uso de credenciales compartidas entre distintos clientes o entornos gestionados por el proveedor

9. Causas raíz y consecuencias: Relación estructural

Los hallazgos del análisis convergen en tres brechas estructurales interdependientes, que se refuerzan mutuamente:

La ausencia de inventarios de activos (no es posible gestionar aquello que no se conoce), la inexistencia de un proceso de gestión de vulnerabilidades (no se corrige lo que no se identifica ni se monitorea), y la falta de controles mínimos de configuración (como autenticación robusta, encabezados de seguridad y mecanismos de autenticación multifactor). La persistencia de cada una de estas brechas amplifica el impacto de las demás y facilita su permanencia en el tiempo.

Las consecuencias documentadas derivadas de esta relación estructural son directas y observables, datos de ciudadanos en circulación en mercados criminales, riesgos relevantes para la continuidad de servicios clínicos, deterioro de la confianza institucional, y exposición prolongada de información sensible, la cual no puede ser recuperada una vez exfiltrada.



Fuente: Construcción Propia

10. El Factor Humano: Vectores no técnicos de riesgo

La ciberseguridad no constituye un desafío exclusivamente técnico. El comportamiento del personal y las prácticas organizacionales pueden amplificar o mitigar de forma significativa el riesgo asociado a las debilidades técnicas existentes. Los vectores humanos que se describen a continuación se habilitan directamente a partir de las brechas estructurales identificadas o son aprovechados de manera complementaria por los actores maliciosos durante los compromisos analizados.

Vector de riesgo	Probabilidad	Mecanismo de explotación	Medida de mitigación
Phishing con datos reales exfiltrados	MUY ALTA	Con nombres, correos institucionales y datos de salud en manos de atacantes, el spear phishing alcanza tasas de éxito >70%.	Capacitación obligatoria. Simulacros periódicos.
Reutilización de contraseñas	ALTA	Una contraseña filtrada se prueba automáticamente contra correo institucional, banca y plataformas nacionales.	Gestor de contraseñas corporativo. MFA como segunda capa.
Software instalado sin controles	ALTA	La ausencia de controles de endpoint permite instalación de malware y herramientas de acceso remoto en equipos institucionales.	Política de software autorizado (whitelist). EDR.
Documentos sensibles en canales inseguros	ALTA	Uso de WhatsApp, correo personal o almacenamiento en nube sin cifrado para compartir documentos reservados.	Clasificación de información obligatoria. Canales aprobados.
Ingeniería social post-filtración	ALTA	Con datos completos de funcionarios (cargo, área, jefe directo), los atacantes construyen pretextos de alta credibilidad.	Verificación de identidad en solicitudes de acceso.

11. Recomendaciones por fase de implementación

La evidencia recopilada confirma que una brecha de seguridad materializada puede representar un costo entre diez y cien veces superior a la inversión preventiva necesaria para evitarla. En el contexto de la campaña analizada, los controles que habrían mitigado los principales vectores de compromiso, incluía la aplicación de parches críticos que no implicaban costos de licenciamiento, sino decisiones oportunas de priorización, ejecución y seguimiento.

Fase 1: Acciones de impacto inmediato

1. Forzar cambio masivo de contraseñas predeterminadas en todas las plataformas institucionales. Esta acción cierra el vector más frecuentemente explotado y tiene costo operativo cercano a cero.

2. Verificar y restringir el acceso a paneles de administración web (/admin/, /wp-admin/, /login/) para que no sean accesibles desde internet sin VPN o lista blanca de IPs.

3. Ordenar un inventario completo de activos tecnológicos: qué software, en qué versión, está en producción. Sin inventario no es posible gestionar vulnerabilidades. Esta es la condición previa de todo lo demás.

4. Aplicar los parches de seguridad disponibles para Moodle, Joomla, WordPress, GLPI y sistemas de gestión. Priorizar CVEs con puntuación CVSS superior a 9.0.

5. Revocar y rotar todas las credenciales de sistemas comprometidos o potencialmente comprometidos, incluyendo credenciales de APIs, conexiones de base de datos y accesos de proveedores externos.

Fase 2: Acciones estratégicas

- Implementar MFA obligatorio: primero para cuentas de administración, luego para todos los usuarios. Google Authenticator y Microsoft Authenticator son gratuitos. Esta medida anula el impacto de cualquier filtración de credenciales.
- Contratar evaluación de seguridad activa para los sistemas con mayor superficie de exposición. Identifica vulnerabilidades que el OSINT pasivo no puede confirmar y produce un roadmap priorizado de remediación.
- Revisar y actualizar contratos con proveedores TI: incluir cláusulas obligatorias de seguridad, SLAs de parcheo y responsabilidad por incidentes derivados de negligencia. Protege a la entidad en caso de compromiso vía cadena de suministro.
- Iniciar migración de plataformas EOL, comenzando con las de mayor criticidad. Sin migración, cada nueva vulnerabilidad descubierta queda abierta permanentemente.
- Implementar inventario de activos y programa de gestión de vulnerabilidades: escaneo continuo, correlación con NVD, priorización por CVSS, SLAs de remediación.

Fase 2: Acciones estratégicas

- SIEM y monitoreo continuo: correlación de eventos de seguridad en tiempo real. Reduce el tiempo de detección de brechas de semanas a horas.
- Plan de respuesta a incidentes (IRP): roles, procedimientos de contención, comunicaciones y recuperación. El patrón de doble incidente en tres entidades confirma que sin IRP la organización repite los mismos errores.
- Concientización obligatoria anual para todos los funcionarios: identificación de phishing, manejo seguro de información y políticas de contraseñas.
- Adopción de un marco de seguridad: NIST CSF 2.0 o CIS Controls v8 para medir la madurez del programa y reportar el estado de seguridad a la alta dirección con métricas objetivas.

12. Servicios de ColCERT disponibles para entidades públicas y privadas

El Equipo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT pone a disposición de las entidades públicas y organizaciones privadas un portafolio de servicios de seguridad digital sin costo alguno, orientado a apoyar la identificación, el análisis y la mitigación de las brechas de seguridad descritas en este informe. Desde 2025, el ColCERT ha ejecutado análisis de seguridad de manera proactiva sobre más de 1.000 entidades públicas y organizaciones privadas en Colombia, contribuyendo al fortalecimiento de capacidades de detección, respuesta y gestión del riesgo digital.

Acceso gratuito: Todos los servicios descritos en esta sección se encuentran disponibles sin costo para entidades públicas y organizaciones privadas. Para solicitar acompañamiento o ampliar información, se encuentra habilitado el canal de contacto contacto@colcert.gov.co.

12.1 Servicios proactivos

El ColCERT desarrolla acciones preventivas orientadas a la identificación temprana de riesgos y debilidades en infraestructuras y servicios expuestos a Internet, con el propósito de reducir la probabilidad de explotación por actores maliciosos. Estos servicios se ejecutan de manera continua y sistemática sobre el conjunto de dominios institucionales colombianos, como parte de las capacidades permanentes de monitoreo y análisis de seguridad.

Servicio proactivo	En qué consiste
Gestión de vulnerabilidades	Identificación de información expuesta en internet: versiones de software vulnerable, endpoints sin autenticación, credenciales filtradas y configuraciones inseguras asociadas a dominios institucionales. Exactamente el tipo de brecha documentada en este informe
Huella digital de la organización	Mapeo de la superficie de exposición pública de la entidad: subdominios activos, servicios expuestos, tecnologías identificables desde fuentes abiertas (OSINT), sin acceso no autorizado a ningún sistema.
Análisis de superficie de ataque	Evaluación de los vectores de entrada disponibles para un actor malicioso, con priorización por nivel de riesgo (CVSS) y recomendaciones concretas de remediación.
Charlas de concientización	Sesiones de formación para funcionarios sobre identificación de phishing dirigido, manejo seguro de información institucional, gestión de contaseñas y buenas prácticas digitales

12.2 Servicios a demanda

De manera complementaria, el ColCERT ofrece servicios especializados que pueden ser solicitados directamente por las entidades, orientados a analizar con mayor profundidad técnica y fortalecer la seguridad de sus sistemas, en función de sus necesidades específicas y nivel de madurez.

Servicio a demanda	En qué consiste
Análisis de vulnerabilidades	Evaluación técnica detallada de los sistemas de la entidad para identificar CVEs sin parchar, configuraciones inseguras y exposiciones de datos. La entidad solicita el servicio y define el alcance con el equipo ColCERT.
Emulación de adversarios	Pruebas controladas de seguridad que simulan el comportamiento de actores maliciosos reales — como los documentados en este informe — para evaluar la capacidad de detección y respuesta de la entidad ante un ataque dirigido.

12.3 ¿Cómo solicitar el acompañamiento?

Las entidades u organizaciones que deseen fortalecer su postura de seguridad digital o acceder a alguno de los servicios descritos pueden contactar directamente al ColCERT. A partir de esta solicitud, el equipo brindará orientación sobre el servicio más adecuado, de acuerdo con el perfil de riesgo, el nivel de madurez y las necesidades específicas de cada organización.

Correo de contacto	Redes sociales
contacto@colcert.gov.co	@colCERT en X (Twitter)

Las brechas documentadas en este informe, incluidas vulnerabilidades sin parchar, configuraciones inseguras, plataformas en estado de fin de vida (EOL) y dependencias de proveedores sin mecanismos de auditoría, corresponden precisamente al tipo de riesgos que el ColCERT cuenta con la capacidad técnica para identificar y frente a los cuales puede orientar a las entidades hacia procesos de remediación efectivos. En este contexto, anticiparse y fortalecer las capacidades internas antes de un compromiso constituye una de las decisiones más relevantes que una organización puede adoptar en el corto plazo.

13. Conclusión: El diagnóstico que No puede postergarse

La campaña de exfiltración que afectó a Colombia entre enero y marzo de 2026 no fue resultado de ataques sofisticados ni de actores con capacidades excepcionales. Los hechos documentados indican que se trató de una consecuencia previsible y evitable, derivada de fallas estructurales persistentes en la gestión de la seguridad digital institucional. En un periodo de semanas, actores con presencia reciente en foros clandestinos lograron comprometer sectores estratégicos, empleando herramientas de libre acceso y explotando vulnerabilidades para las cuales los parches se encontraban disponibles desde meses y en algunos casos, años antes de los incidentes.

La inacción frente a estas brechas tiene un costo tangible y acumulativo, la información exfiltrada de manera permanente, registros de salud e historiales personales de ciudadanos en circulación en mercados criminales, y afectaciones duraderas a la confianza institucional. En este contexto, la pregunta crítica para cada entidad no es si será objetivo de un ataque, la evidencia indica que ya lo es o lo será, sino si, al momento en que ese evento ocurra, existirán controles efectivos capaces de interrumpirlo, o si el atacante encontrará las mismas condiciones de exposición que ya fueron observadas de forma reiterada en múltiples organizaciones del país.

Anexo: Glosario de términos para tomadores de decisión

Los términos técnicos incluidos en el cuerpo de este informe se describen a continuación con el objetivo de asegurar una comprensión precisa y homogénea, sin requerir formación técnica especializada. Esta sección busca facilitar la interpretación de los hallazgos y recomendaciones, apoyando la toma de decisiones informadas a nivel directivo y estratégico.

Término	Definición para tomadores de decisión
CVE (Vulnerabilidad Conocida)	Identificador único de una falla de seguridad documentada en software. Cada CVE tiene un parche disponible. Si una entidad opera software con CVEs sin parchar, el riesgo es conocido, público y evitable.
CVSS 10.0 (Criticidad Máxima)	Escala de 0 a 10. CVSS 10.0 significa que la vulnerabilidad puede ser explotada remotamente, sin credenciales, sin interacción del usuario, con impacto total sobre el sistema. Log4Shell tiene CVSS 10.0 y hospitales colombianos siguen expuestos.
EOL (Fin de Vida)	Software cuyo fabricante dejó de publicar actualizaciones de seguridad. Sin migración, cada nueva vulnerabilidad descubierta queda abierta permanentemente. Equivalente a operar un vehículo sin posibilidad de repararlo.
RCE (Ejecución Remota de Código)	Vulnerabilidad que permite a un atacante ejecutar cualquier código en el servidor remoto sin acceso físico. Equivale a entregar el control total del servidor al atacante.
OSINT (Fuentes Abiertas)	Información obtenida exclusivamente de fuentes públicas y legales: Google, registros DNS, bases de datos de certificados, Shodan, documentos publicados por las propias instituciones.
MFA (Autenticación de Dos Factores)	Además de la contraseña, requiere un segundo factor (código SMS o app). Elimina prácticamente el riesgo de acceso con credenciales robadas. Herramientas como Google Authenticator son gratuitas.
Ransomware	Malware que cifra todos los datos de un sistema y exige pago para recuperarlos. En salud, puede interrumpir UCI, cirugía y medicación crítica.
Cadena de suministro TI	Riesgo de seguridad derivado de proveedores externos con acceso a sistemas institucionales. Un fallo de seguridad en el proveedor compromete a la entidad cliente sin que ésta tenga control ni visibilidad.
Phishing dirigido (spear phishing)	Correo fraudulento construido con información real y específica de la víctima. Con datos ya exfiltrados, el atacante conoce nombre, cargo, área y proyectos, logrando tasas de éxito superiores al 70%.