REGISTRADURÍA NACIONAL DEL ESTADO CIVIL	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado: 06/06/2017

CONTRATO:	**CONTRATO INTERADMINISTRATIVO ELECTRÓNICO No. 068 DE 2025 RNEC**
CONTRATISTA	UNE EPM TELECOMUNICACIONES S.A.
REPRESENTANTE LEGAL (SI APLICA)	Lizbeth Lucely Robayo Perdigon – C.C. 35.196.374
OBJETO DEL CONTRATO:	Servicios para implementar la Ciberseguridad y Seguridad de la información para la organización y realización de los procesos electorales a llevarse a cabo en las vigencias 2025 y 2026.
CIUDAD:	Bogotá
FECHA DE SUSCRIPCIÓN DEL CONTRATO:	03 de octubre de 2025
FECHA DE INICIO:	10 de octubre de 2025
FECHA DE TERMINACIÓN:	30 de julio de 2026
INFORME NRO.	4
PERIODO DE EJECUCIÓN:	01 de enero al 15 de marzo 2026
FECHA PRESENTÉ INFORME:	16 de marzo de 2026

INFORME DE ACTIVIDADES CORRESPONDIENTES AL PAGO NO. 4.

En cumplimiento de cada una de las obligaciones del Contratista, la ejecución y seguimiento por parte de la supervisión del contrato de prestación de servicios No. 068 de 2025 RNEC, para la prestación de servicios en la implementación de la Ciberseguridad y Seguridad de la Información para la organización y realización de los procesos electorales a llevarse a cabo en las vigencias 2025 y 2026. Esta solución debe incluir los pilares que estructuran el servicio: a) Enriquecimiento y contextualización de origen, B) Validación de seguridad automatizada, C) Observabilidad Avanzada, y d) Sistema Integral de Gestión de Riesgos y Cumplimiento.

Generalidades técnicas del servicio

Actualmente, los entornos donde operan los sistemas críticos de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL enfrentan desafíos crecientes en materia de ciberseguridad, especialmente frente a amenazas avanzadas que buscan comprometer la integridad de los procesos electorales. El fortalecimiento de medidas reactivas y proactivas permitirán esclarecer los mecanismos de prevención frente a actores maliciosos que actúan con sofisticación, rapidez y conocimiento del entorno digital. En este contexto, la prevención, visibilidad continua y la inteligencia activa se convierten en pilares fundamentales para garantizar la protección efectiva de la infraestructura electoral.

El servicio Iron Shield for Electoral Integrity tiene como propósito establecer un servicio integral de ciberseguridad (por la vigencia del contrato) orientado a fortalecer, ampliar y sofisticar las capacidades actuales del Centro de Operaciones de Seguridad (SOC), con un enfoque específico en la protección y preservación de la integridad de los procesos electorales.

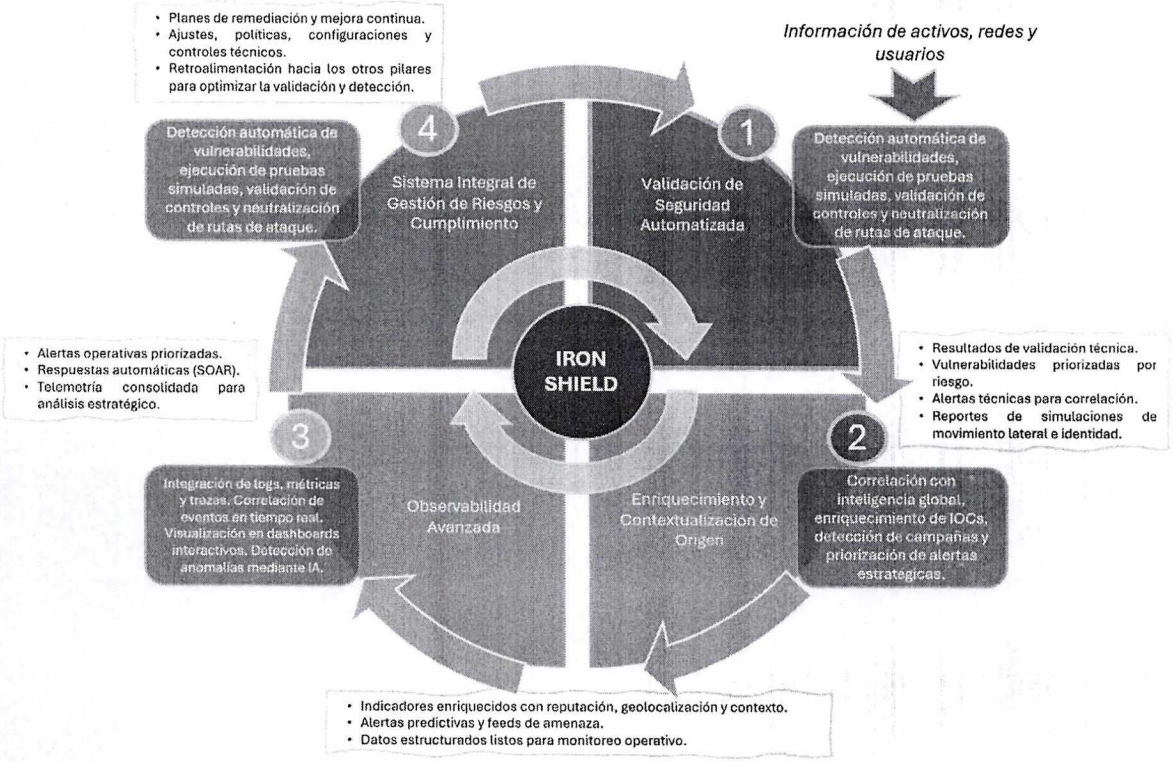
Resumen del servicio:

El servicio Iron Shield for Electoral Integrity tiene como propósito establecer un servicio integral de ciberseguridad orientado a fortalecer, ampliar y sofisticar las capacidades actuales del Centro de Operaciones de Seguridad (SOC), con un enfoque específico en la protección y preservación de la integridad de los procesos electorales.

Este servicio se concibe como una arquitectura funcional que se integra y fortalece los procesos y procedimientos establecidos en Centro de Operaciones de Seguridad (SOC) actual, soportada en cuatro pilares estratégicos, cuya operación será articulada por un equipo interdisciplinario especializado, encargado de ejecutar las actividades

asociadas a cada componente de manera coordinada. El modelo de servicio está diseñado bajo una visión holística, en la cual los pilares no operan como unidades aisladas, sino como partes complementarias de una única solución integral, orientada a la anticipación, mitigación y respuesta efectiva frente a amenazas cibernéticas.

Estructura del Servicio Iron Shield for Electoral Integrity



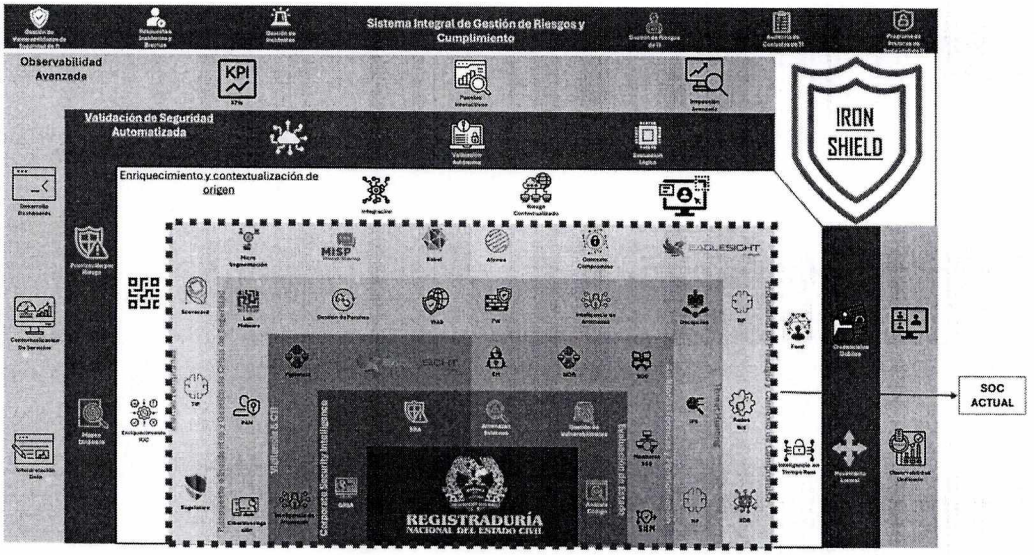
Objetivos del Servicio:

- Fortalecer las capacidades del Centro de Operaciones de Seguridad (SOC), ampliando y sofisticando su infraestructura y procesos mediante una arquitectura integral diseñada para proteger la integridad de los procesos electorales. Este fortalecimiento permitirá mejorar la detección, análisis y respuesta ante incidentes cibernéticos, consolidando una operación más resiliente frente a amenazas avanzadas y garantizando la continuidad de los servicios críticos asociados al ejercicio electoral.

- Transformar la información relacionada con amenazas en inteligencia procesable, integrando fuentes abiertas (OSINT) y datos externos que permitan identificar en tiempo real comportamientos maliciosos, direcciones IP involucradas en ataques y campañas dirigidas contra infraestructuras electorales. Este enfoque de enriquecimiento y contextualización de origen facilita la detección temprana de actividades sospechosas y de actores maliciosos que operen en entornos clandestinos, anticipando acciones preventivas más efectivas.

- Garantizar una Observabilidad avanzada de toda la infraestructura tecnológica, mediante la recolección e interpretación de datos provenientes de múltiples fuentes, tales como Netflow, Syslog, SNMP, API o flujos cifrados. Esta visibilidad permitirá detectar amenazas avanzadas, como movimientos laterales dentro de las redes, correlacionar eventos del SIEM con indicadores de compromiso y acelerar los procesos de investigación y priorización de incidentes, optimizando la respuesta operativa y forense del SOC.

- Implementar un sistema de validación de seguridad automatizada que permita realizar pruebas de penetración continuas, simulaciones de ataques reales y automatización de escenarios de intrusión. Esta capacidad permitirá identificar vulnerabilidades críticas antes de que sean explotadas por actores maliciosos, emulando comportamientos adversarios para fortalecer de manera proactiva la postura de seguridad institucional y garantizar la integridad de los sistemas electorales.



El gráfico describe la relación de los diferentes servicios dentro de la organización y como se interrelacionan con estos cuatro nuevos pilares, que aportan a la seguridad de la información

EVOLUCIÓN DEL SERVICIO / AVANCES

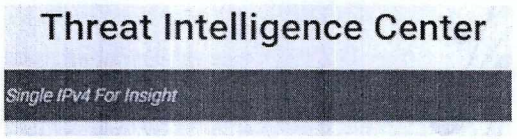


1. ENRIQUECIMIENTO Y CONTEXTUALIZACIÓN DE ORIGEN

1.1 RESUMEN DE LA OPERACIÓN CON LOS HALLAZGOS TÉCNICOS

El servicio de Enriquecimiento y Contextualización de Origen es de valor estratégico para el análisis forense y preventivo por las funcionalidades de 'IP Reputation' e 'IP Insights'. Este tipo de herramientas permiten transformar una simple dirección IP en inteligencia procesable, ofreciendo la capacidad de investigar, clasificar y actuar frente a orígenes sospechosos en tiempo real. Al analizar el historial de comportamiento y asignar puntuaciones de riesgo dinámicas a cada conexión, los equipos de seguridad pueden identificar actores maliciosos basándose en su "reputación" previa en la red global, antes de que logren ejecutar un ataque.

Durante el último periodo la plataforma de enriquecimiento y contextualización de origen ha procesado un total de 96.562 consultas de direcciones IPv4, una cifra que refleja una actividad constante de monitoreo y respuesta ante posibles amenazas. Este proceso de enriquecimiento permite transformar una dirección IP aislada en inteligencia accionable, proporcionando contexto crítico sobre el origen geográfico y la reputación de los activos que interactúan con la infraestructura de la Entidad.

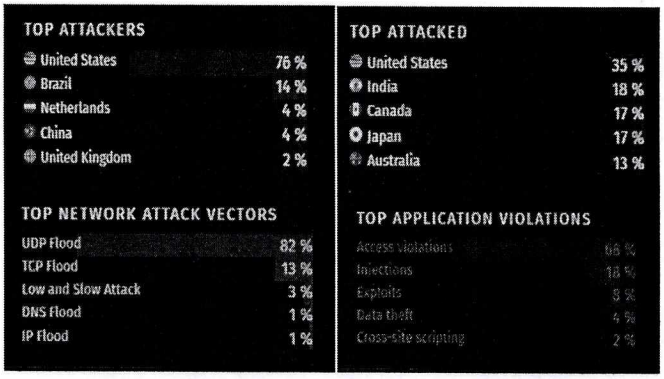


El gráfico describe la relación de consultas.

El uso de esta herramienta ha sido fundamental para fortalecer los procesos de investigación del SOC-CERT, teniendo una cantidad de consultas durante este perido de **146.172** y permitiendo un triage de incidentes mucho más ágil y preciso. Al identificar de forma proactiva aquellas IP's catalogadas como de "alto riesgo" por interceptores globales, los analistas pueden priorizar las alertas que realmente representan un peligro inminente, reduciendo el ruido operativo y el tiempo medio de respuesta (MTTR). Esta capacidad de contextualización actúa como un filtro de seguridad avanzado, asegurando que cada investigación cuente con el respaldo de datos técnicos actualizados y contrastados.

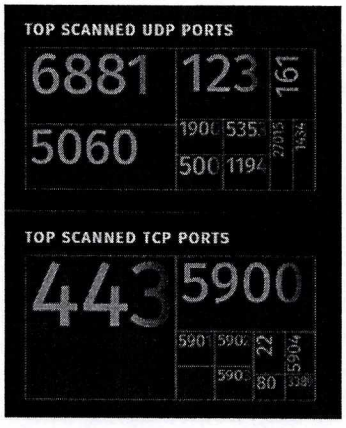
La serie de TOPs que se obtienen en el Live Threat Map permite identificar la actividad de ciberataques a nivel global, dando una visual general sobre ciberamenzas activas, donde se evidencia que Estados Unidos protagoniza el top de países más atacantes y

más atacados, lo que se puede originar por el tamaño de la infraestructura tecnológica que tiene el país.



El gráfico describe el listado de los principales países atacantes y países atacados recientemente.

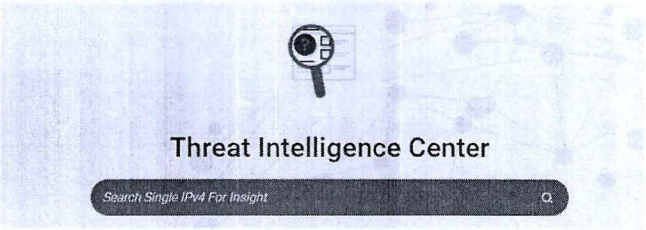
El análisis de los puertos más escaneados revela la fase de reconocimiento de los atacantes, quienes buscan identificar servicios vulnerables o configuraciones por defecto para obtener acceso inicial. En el segmento UDP, destaca el puerto 6.881 (BitTorrent) y el 123 (NTP).



El monitoreo en la red social y aplicación de mensajería instantánea, se refleja una actividad una actividad cibercriminal sumamente intensa durante el periodo comprendido entre el 16 de febrero y el 10 de marzo de 2026. Con un total de 1.044 incidentes adjudicados por solo 23 grupos de atacantes, se observa una alta eficiencia operativa en la ejecución de campañas. El hecho de que se hayan comprometido o reclamado 456 dominios distintos en menos de un mes sugiere que estos grupos

emplean herramientas automatizadas o ataques coordinados a gran escala, utilizando aplicación de mensajería instantánea para el caso Telegram no solo como medio de comunicación, sino como una plataforma de propaganda para validar sus acciones ante su comunidad.

1.2 ACTIVIDADES REALIZADAS A NIVEL TÉCNICO

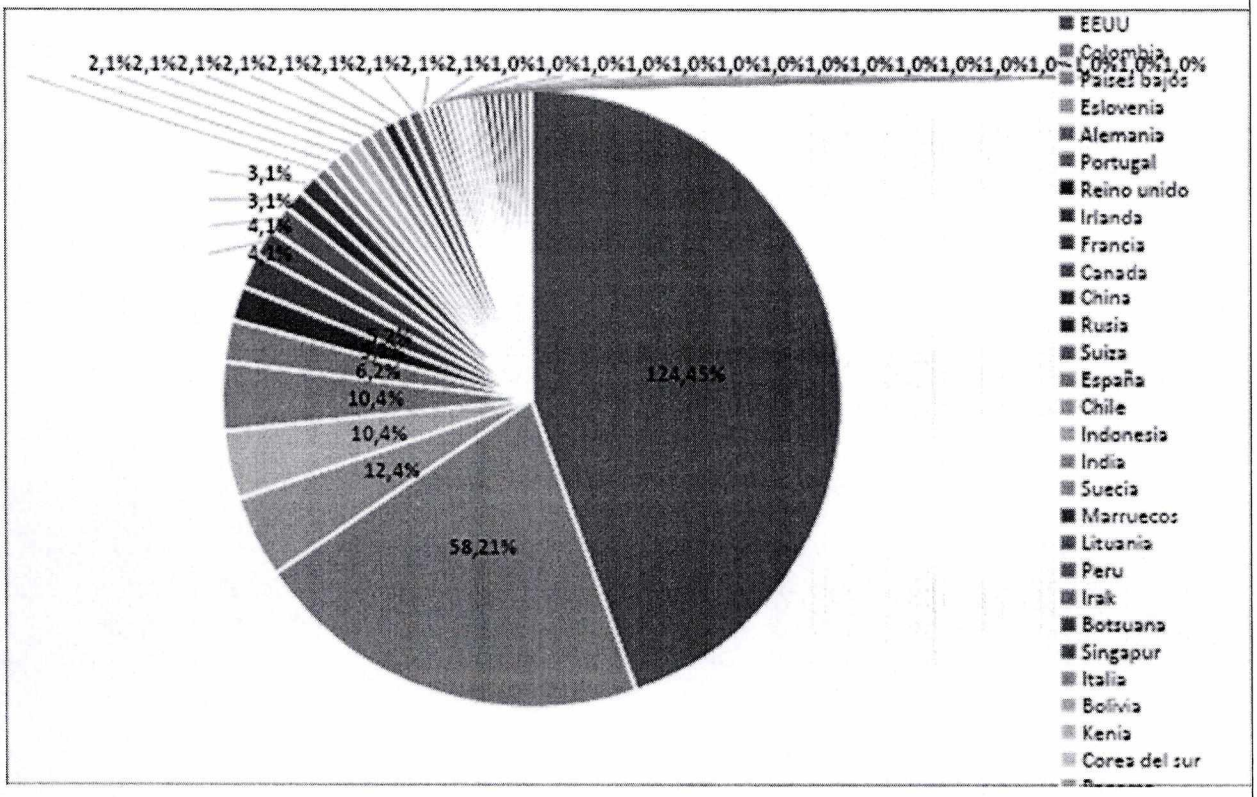


Durante el periodo se consolida el análisis de inteligencia de amenazas y la contextualización forense de las direcciones IP de origen catalogadas como maliciosas, detallando las conexiones entrantes (intentos de intrusión, explotación o escaneo desde el exterior) y salientes (comunicaciones desde la red interna hacia infraestructura hostil) establecidas con la infraestructura tecnológica de la Entidad. Este análisis es crítico, ya que el tráfico entrante representa un intento de ataque activo, mientras que el tráfico saliente sugiere un posible compromiso interna (como comunicaciones a servidores de Comando y Control o exfiltración de datos), permitiéndonos evaluar el vector de ataque, medir el impacto potencial y atribuir la actividad a campañas o actores de amenaza específicos para una respuesta a incidentes más efectiva.

Para el inicio del presente año, se presentó una distribución geográfica de las **278** IP's con indicadores de compromiso analizadas revela una concentración crítica de actividad maliciosa originada principalmente en dos regiones: EE.UU. (45%) y Colombia (21%). Estas ubicaciones juntas representan el 66% del tráfico total identificado, lo que sugiere una exposición focalizada.

Por otro lado, la alta incidencia desde Colombia (21%) plantea un escenario de riesgo por proximidad geográfica y relevancia regional. Este volumen de tráfico puede estar asociado a campañas de phishing dirigidas o al uso de redes de dispositivos locales comprometidos, diseñados para explotar el contexto comercial y cultural de la organización. Esta dualidad entre ataques masivos desde la nube y ataques dirigidos regionalmente eleva significativamente el riesgo de amenazas persistentes, obligando

a la organización a mantener una postura defensiva que sea tanto global como localmente sensible.



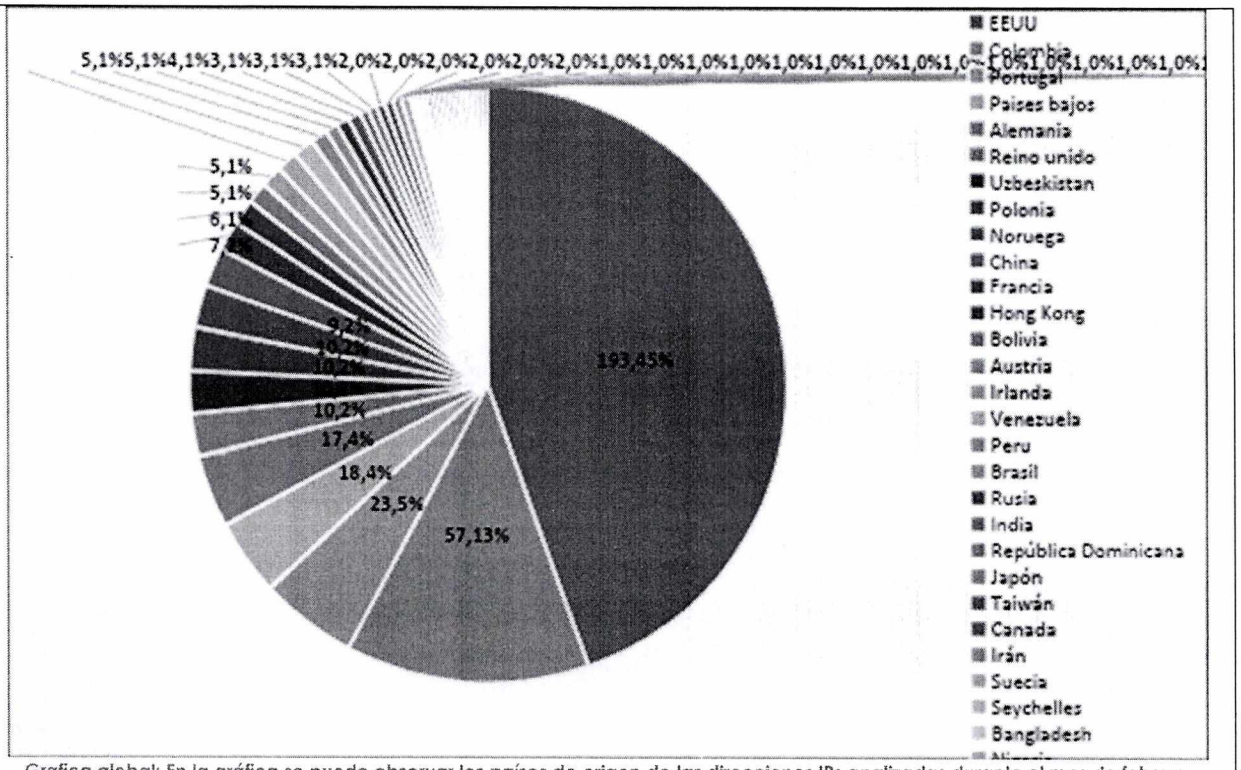
Grafica global: En la gráfica se puede observar los países de origen de las direcciones IPs analizadas durante el mes de enero.

En cuanto al 34% restante, se observa una fragmentación del riesgo con una dispersión global que incluye potencias tecnológicas como Países Bajos, Alemania y China. Esta diversidad geográfica indica que la organización está en el radar de infraestructuras de ataque variadas, incluyendo el uso de nodos de salto y servidores proxy para ocultar el origen real de la intrusión. La presencia de estas conexiones sugiere un nivel de sofisticación técnica donde los atacantes buscan evadir los controles de seguridad perimetral mediante el enmascaramiento de su identidad digital a través de múltiples jurisdicciones.

Para el segundo mes del año, la distribución geográfica de las **433** IP's con indicadores de compromiso analizadas resalta de manera predominante Estados Unidos con un 45% del total (193 IP's). Esta alta concentración suele estar vinculada a que los atacantes utilizan infraestructura de grandes proveedores de servicios en la nube (como AWS, Azure o Google Cloud) o nodos de salida de VPN ubicados en ese país para enmascarar su origen real. Es como si un intruso usara una máscara muy común para intentar pasar desapercibido en una multitud; el hecho de que provengan de EE. UU. no significa necesariamente que el atacante esté allí, sino que está aprovechando la robusta infraestructura tecnológica de esa región para lanzar sus operaciones.

La presencia de Colombia con un 13% (57 IP's) esta cifra sugiere dos escenarios posibles: o bien se trata de tráfico interno comprometido que está intentando comunicarse hacia afuera, o son ataques dirigidos localmente que buscan explotar la cercanía geográfica para evadir ciertos controles básicos. La dispersión en otros países como Portugal (5%), Países Bajos (4%) y Alemania (4%), junto con apariciones de regiones como Uzbekistán, Polonia y China, refleja una amenaza de carácter global y posiblemente automatizada. Muchos de estos países son conocidos por albergar centros de datos con políticas de privacidad estrictas o redes de bots (botnets) que realizan escaneos masivos en busca de vulnerabilidades.

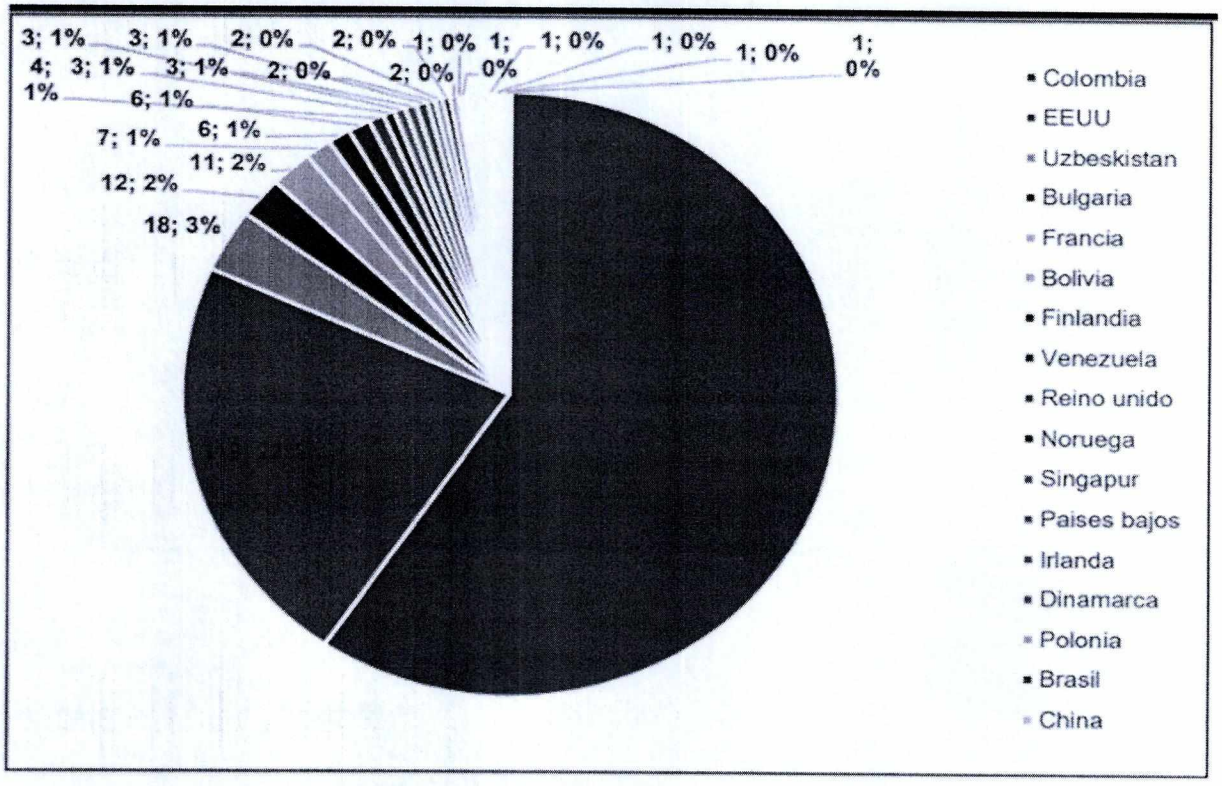
La distribución por niveles de criticidad revela un panorama de riesgo considerablemente elevado, donde la gran mayoría de las comunicaciones detectadas no son simples anomalías, sino amenazas confirmadas. Con un 67% de direcciones IP's clasificadas como de criticidad "Alta" (290 casos), es evidente que la Entidad está siendo blanco de actores o infraestructuras con un historial probado de actividad maliciosa. Estas IP's probablemente corresponden a centros de comando y control (C2), servidores de distribución de malware o nodos activos de redes de ransomware que requieren un bloqueo inmediato y una revisión de logs para descartar filtraciones ya ocurridas.



Grafica global: En la gráfica se puede observar los países de origen de las direcciones IPs analizadas durante el mes de febrero.

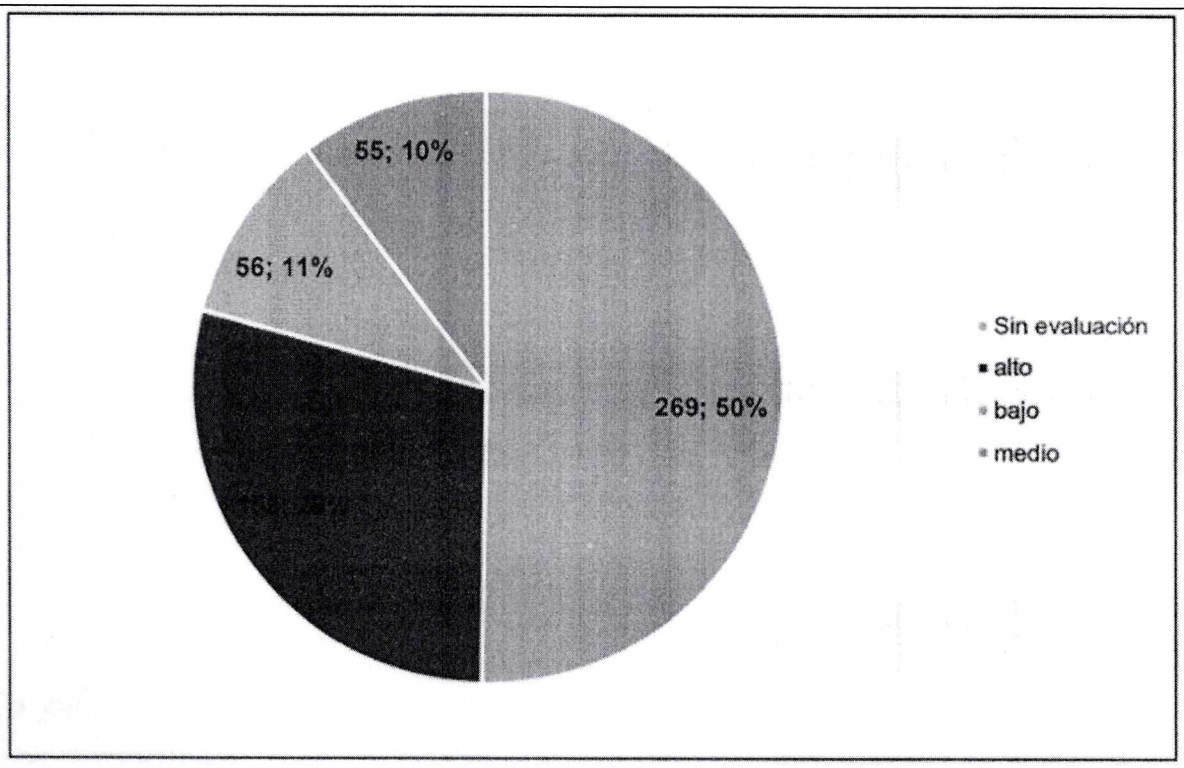
Para el presente mes, dentro del proceso de monitorización se han identificado 535 IP's maliciosas que se han comunicado con la Entidad de las cuales el 59% corresponde a origines en Colombia y un 22% con origen en Estados Unidos.

La alta incidencia de IP's locales es un hallazgo de alta sensibilidad, ya que sugiere que los atacantes están utilizando infraestructura nacional comprometida para evadir controles de geolocalización básicos, los cuales suelen ser más permisivos con el tráfico doméstico en comparación con el tráfico transcontinental.



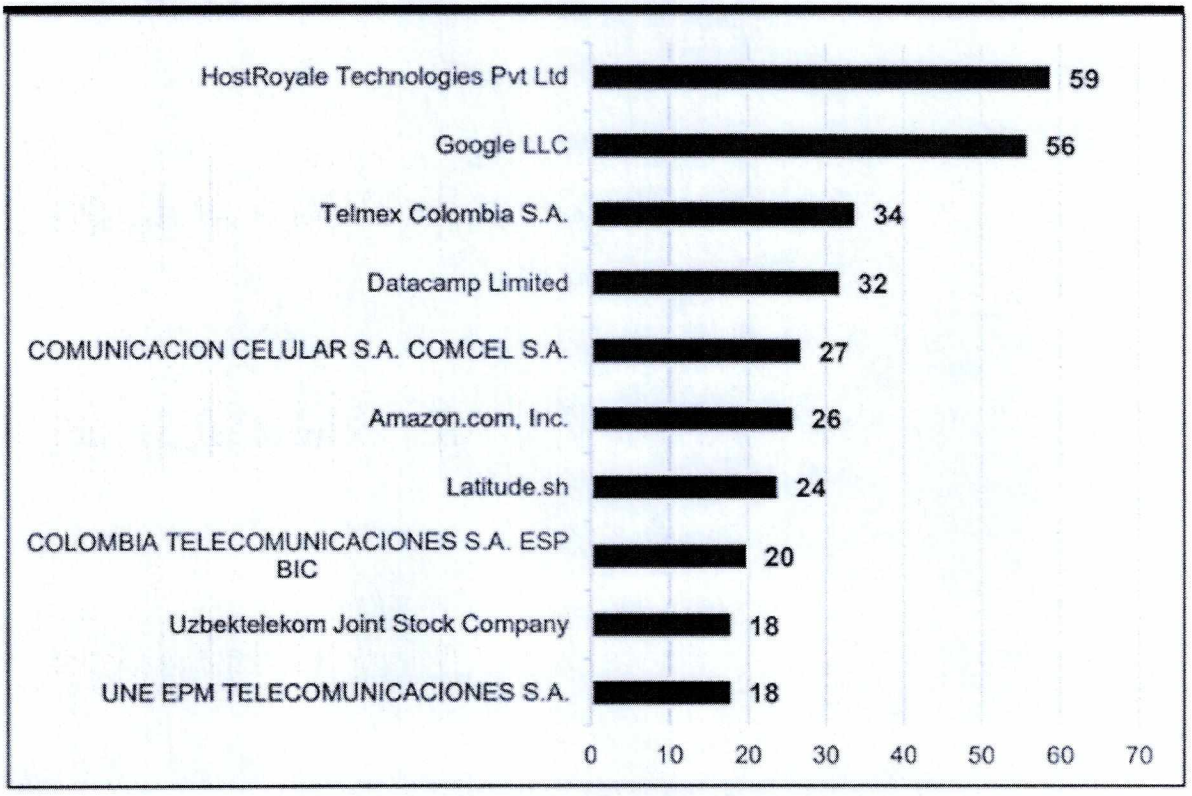
Grafica global: En la gráfica se puede observar los países de origen de las direcciones IPs analizadas durante el mes de marzo

La distribución por niveles de criticidad revela que el 50% de las direcciones IP's (269 casos) categorizadas como "Sin evaluación", son un indicio de que la Entidad se encuentra ante un escenario de incertidumbre técnica donde la mitad de las comunicaciones con indicadores de compromiso no han sido cualificadas.



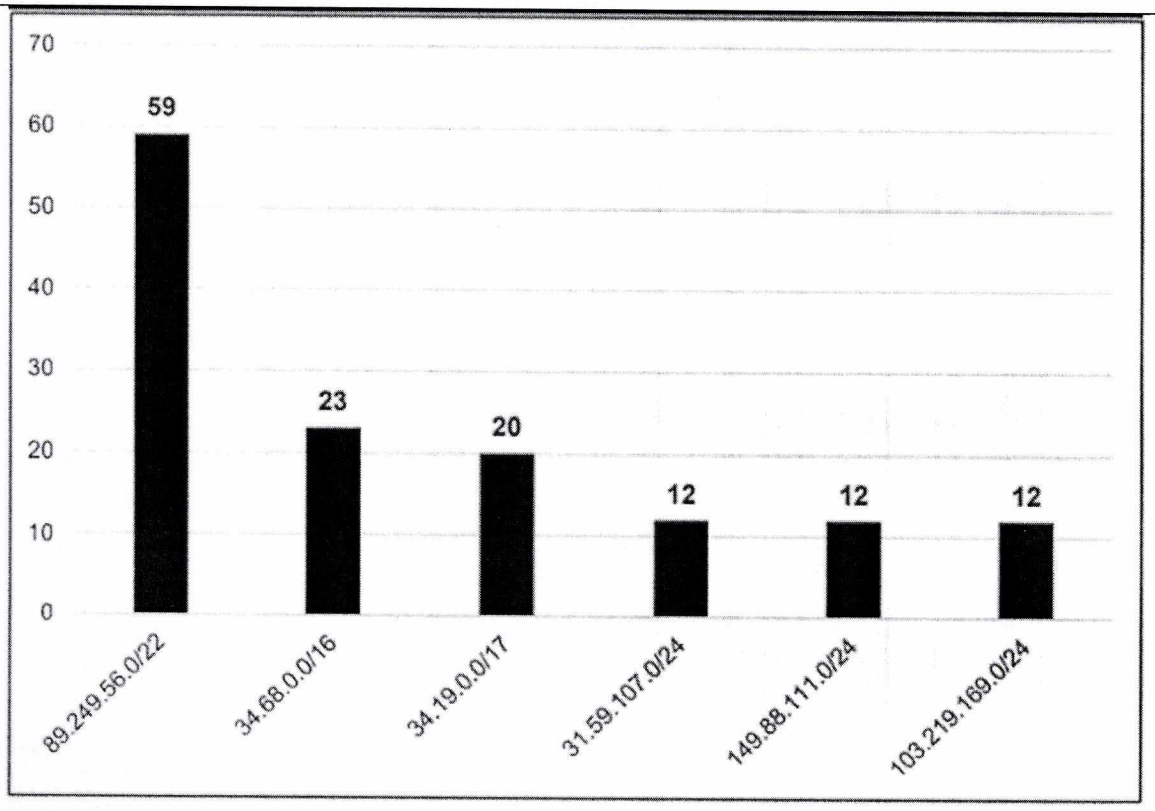
Grafica de distribución por niveles de criticidad.

Al analizar el top 10 de propietarios de IP se evidencia la predominancia de HostRoyale Technologies Pvt Ltd (59 IP's) y Datacamp Limited (32 IP's) lo que es un indicador técnico de peso; estas organizaciones son proveedores de Servidores Privados Virtuales (VPS) e Infraestructura como Servicio (IaaS) que frecuentemente son utilizados por actores de amenazas para desplegar nodos de ataque efímeros o servidores de Comando y Control (C2).



Grafica del top 10 de propietarios de IP

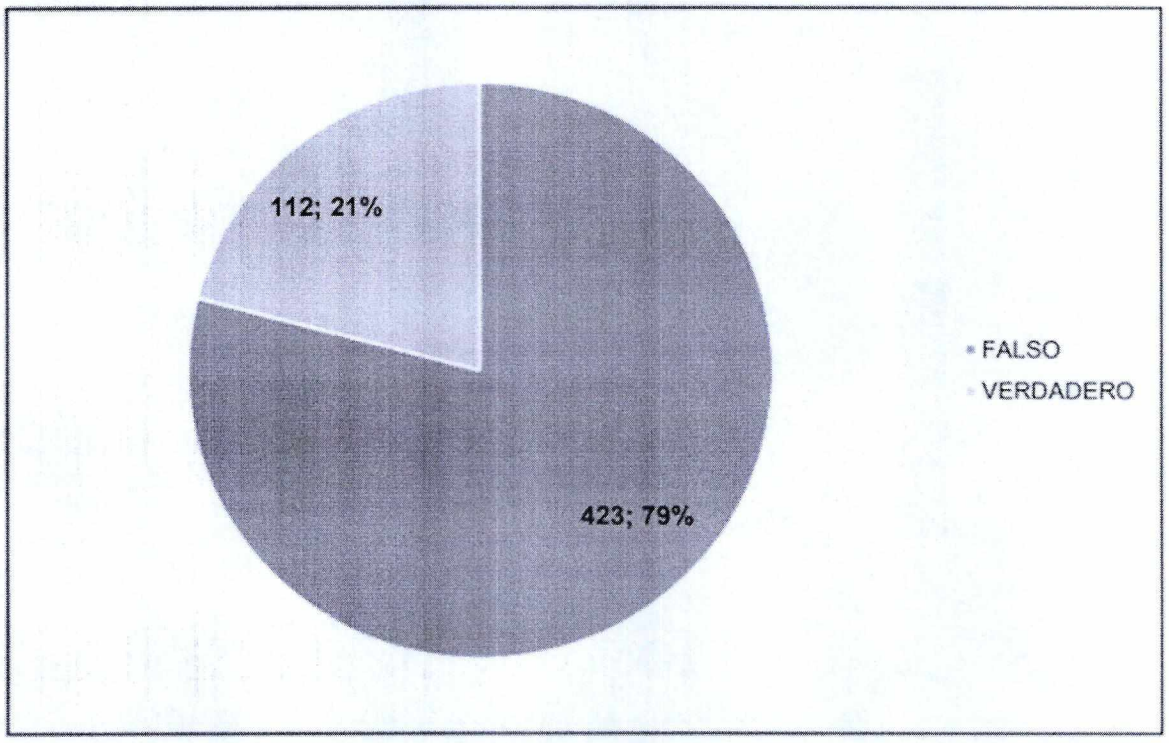
El top 6 de segmentos de red revela una concentración crítica de amenazas provenientes de infraestructuras específicas, destacando el segmento 89,249,56,0/22 con 59 direcciones IP's identificadas. Este hallazgo es técnicamente relevante debido a que la densidad de IP's maliciosas en un bloque relativamente pequeño (/22 equivale a 1,024 direcciones) sugiere una explotación sistemática de este rango, probablemente vinculado a la infraestructura de HostRoyale mencionada anteriormente.



Grafica del top 6 de segmentos de red

Los segmentos 34.68.0.0/16 (23 IP's) y 34.19.0.0/17 (20 IP's) representan una amenaza de naturaleza distinta, al estar asociados a rangos masivos de Google Cloud Platform. La presencia de múltiples incidentes en bloques tan extensos especialmente en un /16 que alberga más de 65,000 direcciones indica que los atacantes están utilizando instancias de cómputo efímeras para lanzar sus actividades.

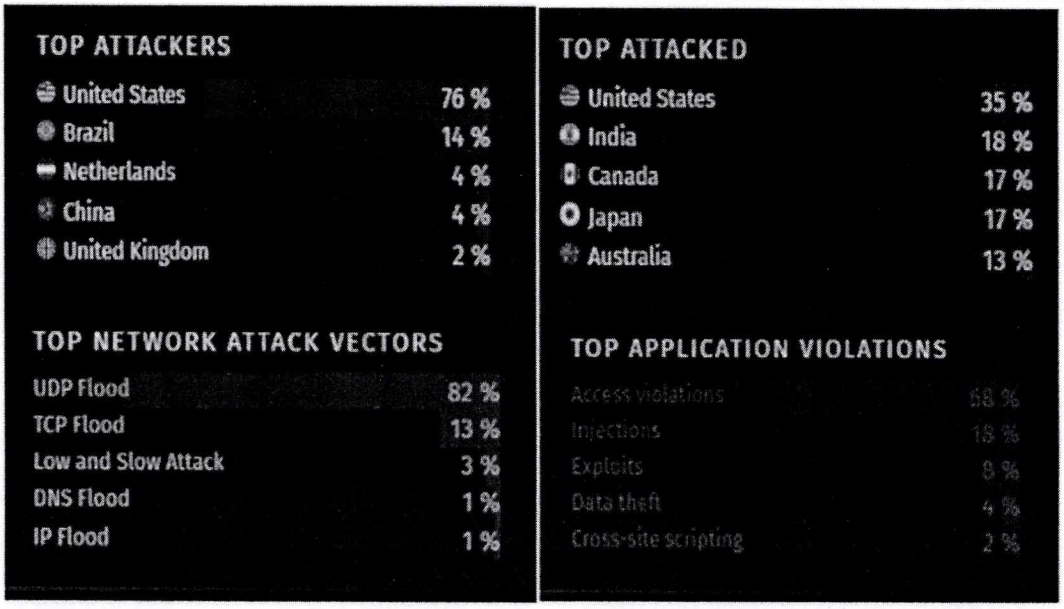
El hallazgo de que el 21% de las direcciones IP's (112 direcciones) pertenecen a botnets confirmadas constituye una validación técnica de que la Entidad está siendo objetivo de ataques automatizados y coordinados. La pertenencia a una botnet indica que estos activos operan bajo una estructura de Comando y Control (C2), lo que aumenta exponencialmente el riesgo de ataques distribuidos, como denegación de servicio (DDoS), campañas masivas de phishing o escaneos de vulnerabilidades a gran escala.



Grafica de botnets confirmadas

Por otro lado, el 79% de las IP's (423 direcciones) clasificadas como "Falso" en su pertenencia a botnets no debe interpretarse como tráfico seguro o legítimo. En el contexto de los análisis previos, donde el 50% de las IP's carecían de evaluación de criticidad, este porcentaje probablemente agrupa a atacantes independientes, servidores comprometidos de forma aislada o infraestructura de ataque emergente que aún no ha sido indexada en las listas de reputación de botnets conocidas.

Mediante el uso Live Threat Map, se evidencio que, el 79% de las IP's (423 direcciones) clasificadas como "Falso" en su pertenencia a botnets no debe interpretarse como tráfico seguro o legítimo. En el contexto de los análisis previos, donde el 50% de las IP's carecían de evaluación de criticidad, este porcentaje probablemente agrupa a atacantes independientes, servidores comprometidos de forma aislada o infraestructura de ataque emergente que aún no ha sido indexada en las listas de reputación de botnets conocidas.



Grafica listado principales países atacantes

Por otro lado, el top de vectores de ataque evidencia un predominio absoluto del UDP Flood con un 82% como vector de ataque principal revela una clara tendencia hacia ataques volumétricos masivos y de baja complejidad técnica, pero de altísimo impacto operativo. Al ser el protocolo UDP (User Datagram Protocol) de naturaleza "sin conexión".

En cuanto a los Puertos TCP, el puerto 443 (HTTPS) domina el gráfico, lo cual es lógico dado que casi todo el tráfico web moderno está cifrado. Sin embargo, este escaneo no busca solo "páginas web", sino vulnerabilidades en las capas de transporte (TLS) o debilidades en aplicaciones web específicas que residen tras ese puerto.

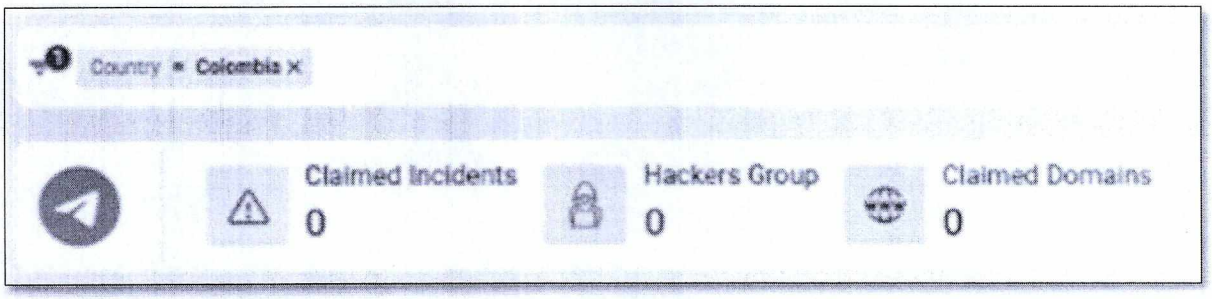


Grafica escaneo puertos TCP

Resulta alarmante observar el bloque dedicado a la familia del puerto 5900 (VNC) y el 3389 (RDP). Estos son objetivos relevantes para el despliegue de Ransomware.

Finalmente, dentro del monitoreo en la red social y aplicación de mensajería instantánea, se refleja una actividad, al analizar el escenario específico para Colombia durante el periodo del 16 de febrero al 10 de marzo de 2026, se observa un contraste absoluto respecto al panorama global gubernamental analizado previamente. En este caso, la herramienta registra cero incidentes reclamados, cero grupos de hackers activos y cero dominios afectados en los canales de Telegram bajo vigilancia.

Esta ausencia de registros indica que, durante esta ventana de tiempo específica, el país no fue un objetivo prioritario para los grupos de hacktivismo y ciber-propaganda (como NoName057 o Desinformador ruso) que suelen utilizar estas plataformas para anunciar sus ataques de denegación de servicio o filtraciones.



Grafica monitoreo en la red social y aplicación de mensajería instantánea – Colombia

1.3 ANÁLISIS DE RESULTADOS OBTENIDOS

El aspecto más crítico para la postura de seguridad actual es la brecha de visibilidad identificada en el análisis de criticidad y recomendaciones, donde un 50% de las IP's carece de evaluación y un 35% permanece sin una acción clasificada. Esta incertidumbre técnica sobre la mitad de los activos detectados representa un riesgo latente, ya que impide la automatización de la defensa y obliga a una gestión reactiva. Es importante priorizar el enriquecimiento de inteligencia sobre este segmento "No clasificado", puesto que la coexistencia de este vacío de información con un 29% de amenazas de alta criticidad indica que la organización está operando bajo un

escenario de riesgo subestimado donde nuevas variantes de ataque podrían estar pasando desapercibidas.

En cuanto a la naturaleza de los ataques, la confirmación de que el 21% de las IP's pertenecen a botnets activas valida la existencia de intentos de intrusión coordinados y automatizados. La estrategia inmediata debe centrarse en la ejecución del bloqueo del 35% de las IP's recomendadas por la herramienta y la implementación de un monitoreo estricto sobre el 29% de activos bajo vigilancia, especialmente aquellos vinculados a segmentos de red específicos como el bloque 89.249.56.0/22. La transición hacia un modelo de defensa proactiva requerirá no solo la mitigación de las amenazas confirmadas, sino también la resolución urgente del estado de las IP's no evaluadas para reducir el tiempo de detección y respuesta ante posibles incidentes de seguridad.

El panorama extraído del monitoreo revela que el hacktivismo de corte geopolítico se ha consolidado como la principal fuerza disruptiva contra la infraestructura pública global. La actividad predominante de colectivos como NoName057(16) y el actor "Desinformador ruso" evidencia una transición hacia operaciones de ciberdefensa y propaganda, donde el objetivo primordial no es el lucro, sino la saturación de servicios estatales para erosionar la confianza ciudadana. Esta dinámica convierte a los canales de Telegram en centros de comando y validación, donde la magnitud de un ataque se mide por su impacto mediático y su capacidad de paralizar portales gubernamentales en momentos de alta tensión diplomática.

La volatilidad en la frecuencia de los incidentes, marcada por repuntes masivos como el observado el 6 de marzo, confirma el uso de redes de botnets altamente automatizadas y con capacidad de despliegue inmediato. Estos picos de actividad demuestran que los atacantes poseen la infraestructura necesaria para ejecutar ofensivas relámpago que desbordan los perímetros de seguridad convencionales. Ante esta realidad, la resiliencia institucional depende de la implementación de sistemas de mitigación dinámicos y elásticos que puedan neutralizar ataques de denegación de servicio en tiempo real, garantizando la disponibilidad de los servicios críticos incluso bajo condiciones de saturación extrema.

Se destaca una asimetría crítica entre el origen y el destino de las amenazas mientras que Estados Unidos concentra la gran mayoría de la actividad saliente debido a su densa infraestructura de nube, la distribución de los objetivos es más diversificada entre potencias económicas como India, Japón y Canadá. Esto confirma que los actores de amenazas están utilizando servidores legítimos en países desarrollados como plataformas de salto para atacar activos de alto valor. En este sentido, la defensa no puede basarse únicamente en el bloqueo por geolocalización, sino que debe

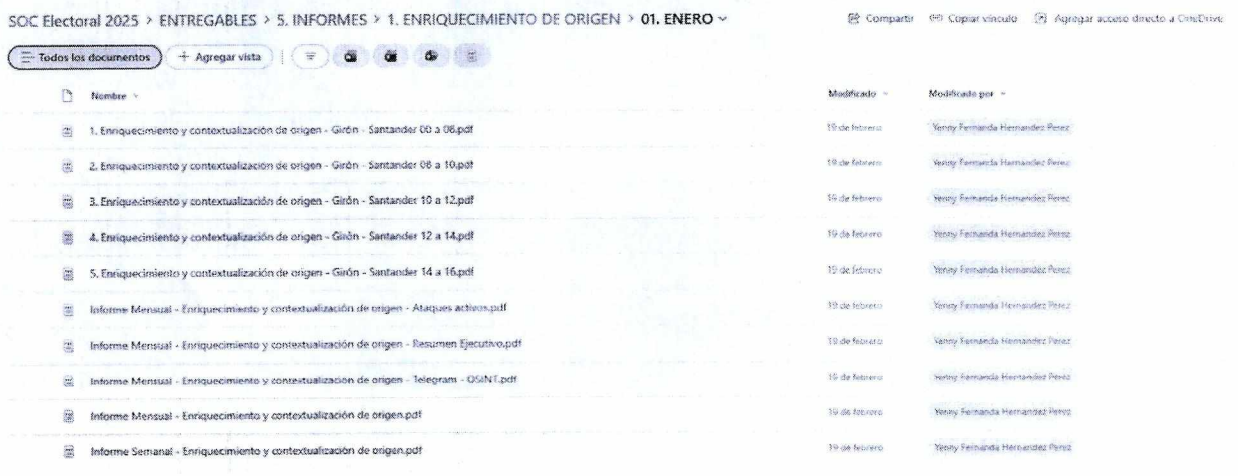
evolucionar hacia una inspección profunda del comportamiento del tráfico, reconociendo que la infraestructura de confianza es hoy el principal vector de anonimato para el atacante.

Respecto al panorama regional y global, es relevante señalar que Colombia no figura en los listados principales de países atacantes ni de países atacados durante este periodo. Esta ausencia sugiere que, aunque el país enfrenta desafíos de ciberseguridad internos, su infraestructura nacional no está siendo utilizada masivamente por redes de botnets globales, ni el país representa actualmente uno de los cinco objetivos prioritarios para ofensivas estatales o de ransomware a gran escala. No obstante, esto no debe interpretarse como una falta de riesgo, sino como una oportunidad estratégica para que las organizaciones colombianas fortalezcan sus posturas defensivas antes de que los cambios en las tendencias geopolíticas o económicas desplacen el interés de los atacantes hacia la región.

El análisis de escaneo de puertos a nivel global subraya que la exposición de servicios de administración remota, como RDP y VNC, sigue siendo fuentes de riesgo para muchas infraestructuras. Los atacantes mantienen un escaneo persistente y automatizado en busca de estos puntos de entrada para el despliegue de ransomware.

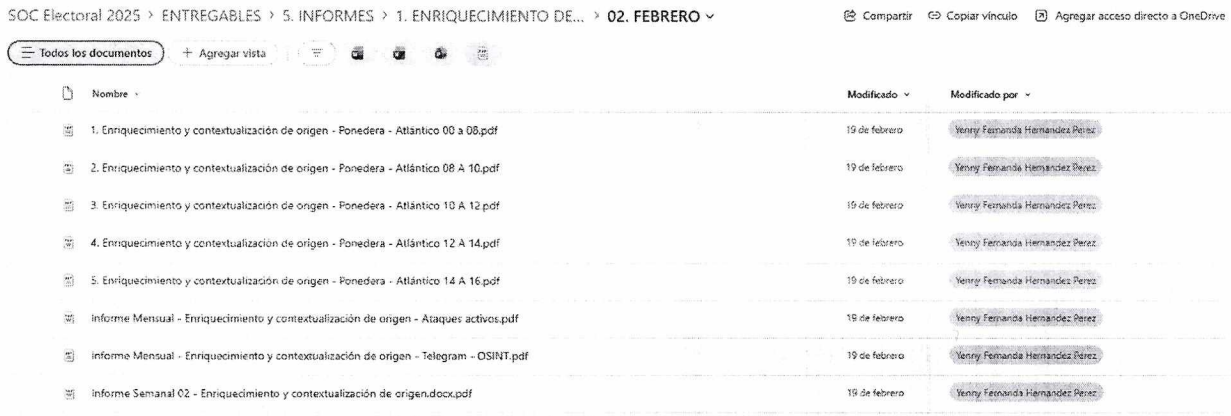
Durante este periodo se ha publicado los siguientes informes, los cuales se encuentran disponibles en la ruta dispuesta para el proyecto.

ENERO



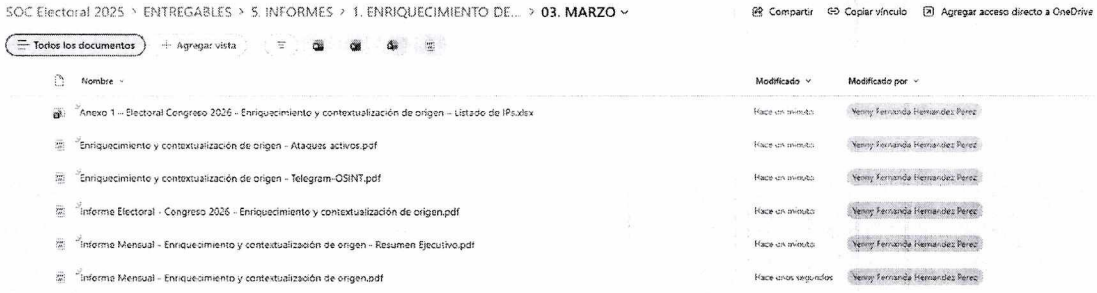
Informes mensuales de la operación del Servicio.

FEBRERO



Informes mensuales de la operación del Servicio.

MARZO



Informes mensuales de la operación del Servicio.

1.4 RECOMENDACIONES TÉCNICAS

Para fortalecer la postura de seguridad de la Entidad frente a los hallazgos detallados en este análisis, se recomienda como medida de contención inmediata la ejecución del bloqueo en el firewall perimetral y en los sistemas de prevención de intrusiones (IPS) de las 188 direcciones IP's que cuentan con una recomendación de bloqueo explícito.

Esta acción debe ser priorizada para neutralizar de manera efectiva el 29% de las amenazas confirmadas como de alta criticidad, reduciendo así la superficie de ataque

frente a vectores ya validados. Es fundamental que estos indicadores de compromiso (IoC) sean integrados en las listas de denegación de forma automatizada para minimizar la ventana de oportunidad de los atacantes y asegurar una respuesta ágil ante la infraestructura maliciosa identificada.

Resulta importante establecer un proceso de enriquecimiento de datos y análisis forense orientado específicamente a resolver la incertidumbre sobre el 50% de las direcciones IP's que actualmente carecen de una evaluación de criticidad. La presencia de este volumen de tráfico no clasificado constituye un riesgo operativo latente que debe ser mitigado mediante la integración de fuentes adicionales de inteligencia de amenazas (Threat Intelligence) y la correlación de logs internos. El objetivo principal debe ser categorizar estos activos para determinar si representan amenazas emergentes o tráfico anómalo que requiera una transición hacia la lista de bloqueo, eliminando así los puntos ciegos en la visibilidad de la red perimetral.

En cuanto a la gestión de la infraestructura, se sugiere aplicar políticas de filtrado basadas en segmentos de red para bloques con alta densidad de incidentes, como el segmento 89.249.56.0/22 vinculado a proveedores de VPS. No obstante, dado que una parte significativa del tráfico proviene de proveedores de nube legítimos y proveedores de servicios de internet (ISP) locales en Colombia, la estrategia de defensa no debe limitarse a bloqueos geográficos o de reputación estática. En su lugar, se recomienda implementar reglas de inspección profunda de paquetes (DPI) y controles de acceso basados en comportamiento (Zero Trust), lo cual permitirá diferenciar con precisión las comunicaciones maliciosas de las actividades legítimas de usuarios y servicios, garantizando la continuidad del negocio sin comprometer la seguridad.

Desde una perspectiva de defensa proactiva, este panorama exige una revisión inmediata de las políticas de acceso perimetral. Dado que el mayor volumen de IoC es local, no basta con aplicar bloqueos geográficos; es imperativo implementar reglas de inspección profunda y límites de tasa de conexión (rate limiting) específicos para el tráfico nacional sospechoso. Se recomienda correlacionar estos datos con los registros de los firewalls y sistemas de detección de intrusiones para identificar si alguna de estas comunicaciones fue exitosa, priorizando la limpieza de cualquier sesión activa proveniente de las IP's identificadas en este reporte para mitigar el riesgo de una brecha de seguridad.

Adicionalmente, para gestionar eficazmente las detecciones de direcciones IP con indicadores de reputación negativos, se recomiendan un enfoque que combine la automatización técnica con la investigación.

Algunas Medidas Técnicas de Contención y Respuesta, que pueden ser implementadas son:

Bloqueo Automatizado en Perímetro: fortalecer reglas de firewall o sistemas de prevención de intrusiones (IPS) para denegar el tráfico entrante y saliente de las IPs identificadas como maliciosas.

Enriquecimiento de Alertas: Utilizar las plataformas de inteligencia, para obtener contexto sobre la IP (geolocalización, historial de ataques, asociación con grupos de amenazas conocidos).

Aplicación de políticas de limitación de tráfico en lugar de un bloqueo total para evitar falsos positivos.

A**islamiento Preventivo:** al detectar comunicación interna hacia una IP de reputación negativa, desconectando el host afectado de la red para evitar el movimiento lateral o la exfiltración de datos.

2. VALIDACIÓN DE SEGURIDAD AUTOMATIZADA

2.1 RESUMEN DE LA OPERACIÓN CON LOS HALLAZGOS TÉCNICOS

El servicio de Validación de Seguridad Automatizada permite, de manera continua, identificar en activos de información evaluados, las vulnerabilidades explotables que se han depurado y priorizado de acuerdo con criterios de seguridad de la información, alineándolos con el estándar MITTRE Attack. El servicio ofrece las siguientes prestaciones:

- Simula de forma automática y continua ataques reales, incluyendo vectores de ataque complejos y cadenas de ataque, en todas las capas de ciberseguridad.
- Se enfoca en vulnerabilidades explotables, malas configuraciones, credenciales filtradas y privilegios excesivos, reduciendo falsos positivos.
- Opera de manera segura, sin comprometer la disponibilidad de los servidores.
- Funciona sin necesidad de instalar agentes en los activos a evaluar.
- Utiliza un motor de ataque algorítmico para generar y probar miles de vectores de ataque.
- Permite ajustar la intensidad de la prueba, entre modo sigilosos o ruidosos.
- Permite ejecutar al instante y programar re-test periódicos.

- Proporciona un plan de acción paso a paso para eliminar las exposiciones de manera efectiva.

De forma complementaria, se cuenta con el componente para evaluación continua del dominio principal y subdominios de regsitraduria.gov.co, el cual permite:

- Mapeo e identificación continuo de superficie externa de ataque usando inteligencia de código abierto OSINT
- Descubrimiento de rutas de ataque externas usando ataques safe-by-design, alineados a OWASP y MITRE ATT&CK, para entender la cadena de eliminación.
- Prioriza y centra esfuerzos de remediación en vulnerabilidades más explotables, clasifica activos más atractivos como lo vería un atacante.

Dentro de los principales hallazgos técnicos, encontramos:

Superficie de ataque externa: Se ha mapeado la superficie de ataque externa con 161 subdominios relacionados a 24 diferentes redes y 197 direcciones IP con 861 servicios publicados, con variaciones incrementales en los períodos de ejecución. Se detectan más de 250 subdominios inactivos cada período.

Credenciales filtradas: Se han descubierto más de 150 credenciales filtradas de cuentas de usuarios pertenecientes a la Entidad, que son utilizados para registrarse en plataformas de entretenimiento y redes sociales principalmente

Vulnerabilidades identificadas: Se han detectado algunas vulnerabilidades relacionadas con uso de wildcard en certificados, bandera HSTSi desactivada y puertos con servicios obsoletos expuestos como FTP y Telnet en algunos subdominios.

Pruebas de concepto Ransomware: Se han realizado pruebas de concepto exitosas que crean copias de archivos, los cifran y luego tratan de exfiltrarlos fuera de la red y después los borran, para comprobar la efectividad de controles cómo XDR y DLP, por ejemplo.

2.2 ACTIVIDADES REALIZADAS A NIVEL TÉCNICO

- La herramienta se encuentra en versión 7.1.5, se instaló en plataforma ESXi, en máquina virtual ubicada en datacenter de RNEC, con sistema operativo Ubuntu Ver. 22.04.
- El reloj interno se ha sincronizado con el Directorio Activo de RNEC, y se activó segundo factor de autenticación 2FA, para todos los usuarios.

- Se cuenta con acceso por protocolo SSH con claves RSA SHA256.
- Se encuentra en fase de implementación un nodo de cracking que será instalado en el mismo segmento de red, conectado al nodo principal.
- El servidor se ubica en VLAN interna, conectada a un puerto troncal del switch core.
- Se han solicitado permisos de conexión hacia las subredes internas de RNEC.
- La máquina tiene acceso autorizado a las URL de actualización de producto del fabricante.
- Tiene una interfaz de administración e interfaces de manejo interno del DOCKER que despliega el fabricante para la herramienta en sí.

Integración con Herramienta de Observabilidad Avanzada: Se generaron tokens de conexión, usuario y contraseña para la integración con herramienta Viewtinet y se realizó la integración usando API y Syslog, para generar estadísticas de uso, disponibilidad y resultados de la validación de seguridad automatizada.

Aseguramiento: Se realizo aseguramiento en el sistema operativo y la aplicación para prevenir fuga de datos y evitar que un potencial atacante aproveche las capacidades de ataque de la herramienta de validación de seguridad automatizada.

Se aplicaron medias de seguridad en los siguientes componentes: Usuario root, Comandos de alto privilegio restringido, Soporte de protocolos de red innecesarios eliminado, Compatibilidad con sistemas de archivos innecesarios desactivada, Desinstalación de paquetes comunes, Volcados de Kernel desactivados, Algoritmo por defecto de contraseñas actualizado, y Política estricta de contraseñas

Copia de respaldo: Se ha creado rutina de creación de copia de respaldo de la máquina virtual de la herramienta, y se han generado copia de respaldo en cada período.

2.3 ANÁLISIS DE RESULTADOS OBTENIDOS

Durante este período, se realizaron pruebas del servicio con diferentes componentes a nivel externo e interno identificando oportunidades de mejora en la gestión y tratamiento de vulnerabilidades.

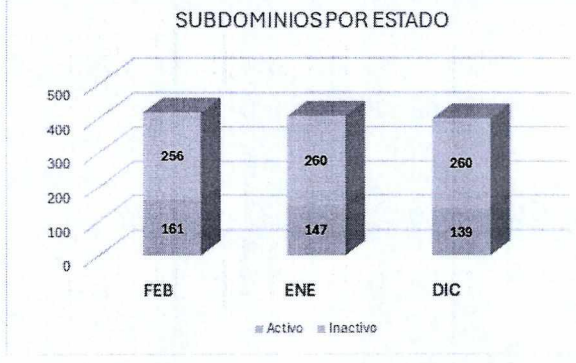
A la fecha se han entregado diferentes documentos asociados al servicio validación automatizada de Seguridad, se está a la espera de retroalimentación por parte del cliente.

La puesta en marcha de pruebas del servicio se ha llevado a cabo con el apoyo de cliente y su proveedor tecnológico, se deben seguir realizando ajustes para que cada componente tenga cobertura total.

Superficie de ataque externa

Se observa una tendencia de crecimiento de los subdominios activos desde diciembre, 5% y 9% mensual. Dado que los subdominios amplían la superficie de ataque, es importante mantener control estricto de las vulnerabilidades que se identifiquen. Para el período actual, se han excluido 260 subdominios que aparecen inactivos, de los totales de la prueba. Los dominios inactivos no están en línea, pero hay que revisar si en un futuro se pueden requerir.

Los Subdominio inactivo es una dirección web secundaria de un dominio principal que no está en uso, no tiene contenido activo o no responde a solicitudes en internet. Registraduría mantiene de forma dinámica, cientos de subdominios que activa o desactiva a demanda, de forma permanente.



Estado	FEB	ENE	DIC
Activo	161	147	139
Inactivo	256	260	260
Total general	**417**	**407**	**399**

Gráfico superficie de ataque externa.

Credenciales filtradas

El servicio de Validación de Seguridad Automatizada utiliza técnicas de OSINT, para mantener de forma automática y continua, simulaciones de ataques reales, incluyendo vectores de ataque complejos en todas las capas de ciberseguridad, identificando debilidades en la infraestructura de seguridad, y funciona sin necesidad de instalar agentes en los activos a evaluar. El foco son vulnerabilidades explotables, malas configuraciones, credenciales filtradas y privilegios excesivos.

Una de las capacidades de este servicio, es identificar en cientos de recursos disponibles en la web profunda, web oscura, buscadores, redes sociales y fuentes abiertas de información, así como inteligencia de amenazas, para descubrir, usuarios, y contraseñas filtradas, basando la búsqueda en un dominio específico.

Este servicio permite obtener una imagen precisa de qué credenciales los atacantes pueden obtener o descifrar para lograr acceso a sistemas de información, plataformas o aplicaciones y tener una idea de qué ataques podrían planear.

Se han encontrado 53 credenciales filtradas en internet consultando diferentes fuentes.

Pruebas de concepto Ransomware

Con periodicidad mensual, se ejecutan pruebas técnicas de validación de seguridad automatizada, con enfoque preventivo y validatorio, orientado a comprobar la eficacia de controles de seguridad informática de detección de malware, concretamente ramsomware, con el fin de fortalecer la resiliencia a amenazas de este tipo. La prueba ejecuta un flujo de ataque de extremo a extremo de una campaña de ransomware.

La simulación controlada imita el comportamiento de ramsomware, incluyendo cifrado de archivos de prueba y generación de alertas similares a las de un ataque real. La emulación no afecta datos productivos, pero permite observar cómo reaccionan las defensas instaladas.

Inicialmente se especifican las extensiones de archivo que serán objeto de la prueba, y la variante específica de ramsomware a utilizar, de las muestras disponibles, luego la herramienta hace una búsqueda de estos archivos en la máquina de destino, crea una copia de ellos, cifra las copias y elimina al final los archivos que haya cifrado y se informa si todo el proceso fue exitoso o fue detenido en algún momento. También es

posible, si se dispone de un servidor de comando y control, exfiltrar la información hacia fuera de la organización para probar controles de fuga de información.

2.4 RECOMENDACIONES TÉCNICAS

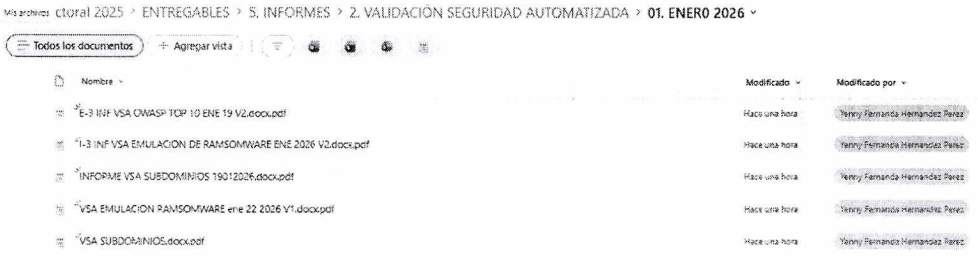
- Se descubrieron puertos cerrados en 70 direcciones IP, se requiere verificar que el firewall esté filtrando el acceso al puerto de forma restringida sólo a direcciones IP autorizadas.
- Se reportó información de tecnologías y configuración de algunos sitios, se requiere verificar si es confidencial.
- 04 sitios web presentan cifrado débil en certificados.
- Un sitio respondió a un ataque genérico de XSS, se requiere una verificación manual para descartar o comprobar la vulnerabilidad.
- 70 sitios web usan certificado comodín se recomienda limitar a subdominios que realmente lo necesitan y considerar certificados individuales para servicios críticos, que reduce el impacto de una posible filtración y usar HSTS y TLS versión 1.3.
- Para acceso remoto al servicio RDP, se recomienda bloquear el acceso público al puerto 3389 mediante firewall, restringiendo conexiones a una lista blanca de direcciones IP conocidas, usar VPN para acceder al servicio, evitando la exposición directa, configurar RDP para escuchar únicamente en redes internas, nunca en la IP pública, habilitar autenticación multifactor para las cuentas que usan RDP y desactivar cuentas por defecto y aplicar contraseñas complejas.
- En las direcciones IP con puertos cerrados verificar que el firewall esté filtrando el acceso al puerto de forma restringida sólo a una lista blanca de direcciones IP autorizadas.
- Reforzar capacitación a usuarios para no utilizar la cuenta de correo institucional para registrarse en otras aplicaciones.

- Reforzar sensibilización en higiene informática para que las credenciales sean de uso exclusivo para fines laborales y evitar la exposición a riesgos de seguridad y reducir la posibilidad de accesos no autorizados.

- Revisar las políticas internas de seguridad relacionadas y verificar que se monitorean con indicadores.

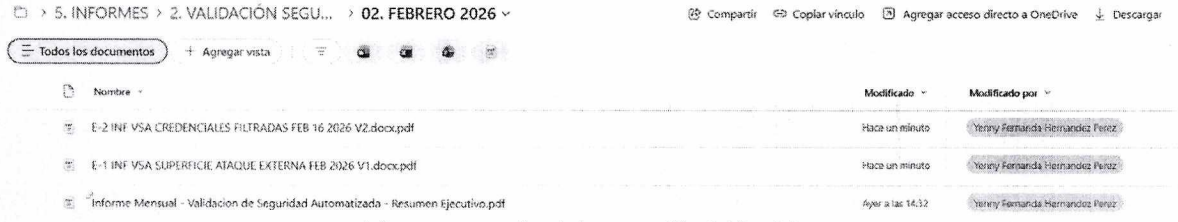
Durante este periodo se ha publicado los siguientes informes, los cuales se encuentran disponibles en la ruta dispuesta para el proyecto.

ENERO



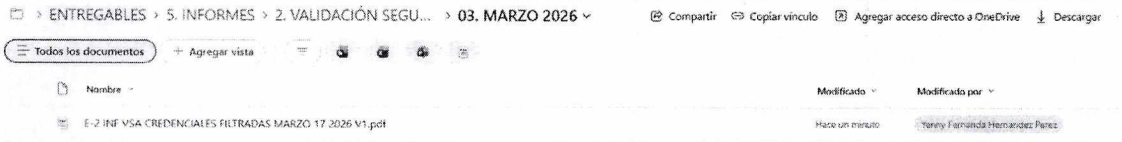
Informes mensuales de la operación del Servicio.

FEBRERO



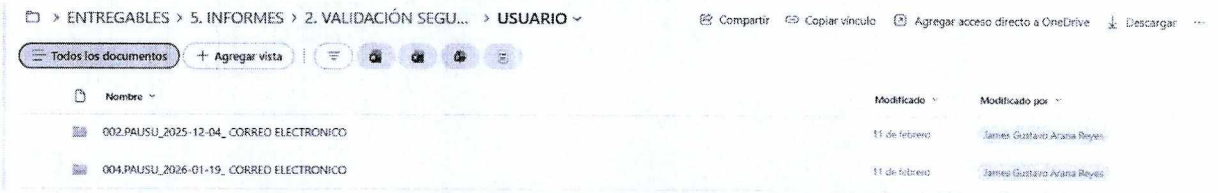
Informes mensuales de la operación del Servicio.

MARZO



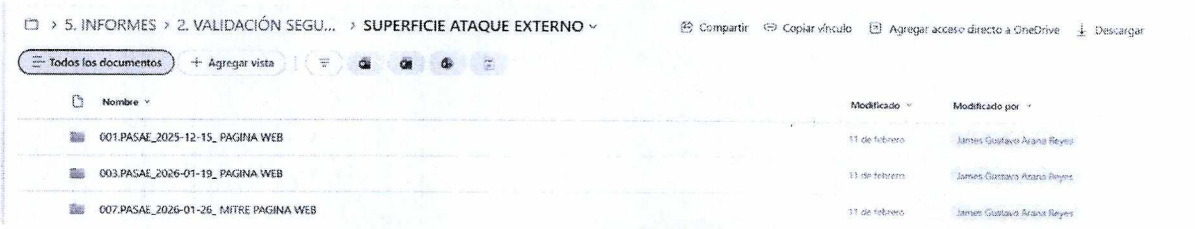
Informes mensuales de la operación del Servicio.

USUARIO



Informes mensuales de la operación del Servicio.

SUPERFICIE DE ATAQUE EXTERNA



Informes mensuales de la operación del Servicio.

3. OBSERVABILIDAD AVANZADA

3.1 RESUMEN DE LA OPERACIÓN CON LOS HALLAZGOS TÉCNICOS

El servicio de observabilidad avanzada propone una solución de monitoreo del rendimiento operativo de los servicios integrados mediante el reporte de métricas de servidores, latencia y estados de salud obtenidos exclusivamente de los servicios que se encuentran bajo la observación del modelo de Observabilidad Avanzada hasta la fecha.

A su vez centralizó la gestión de registros del alcance actual para consolidar eventos provenientes de plataformas con integración activa como FortiGate, Microsoft 365 Defender, AWS CloudTrail y sistemas operativos, limitando la revisión unificada a los registros que ya están siendo procesados por el servicio de Observabilidad Avanzada.

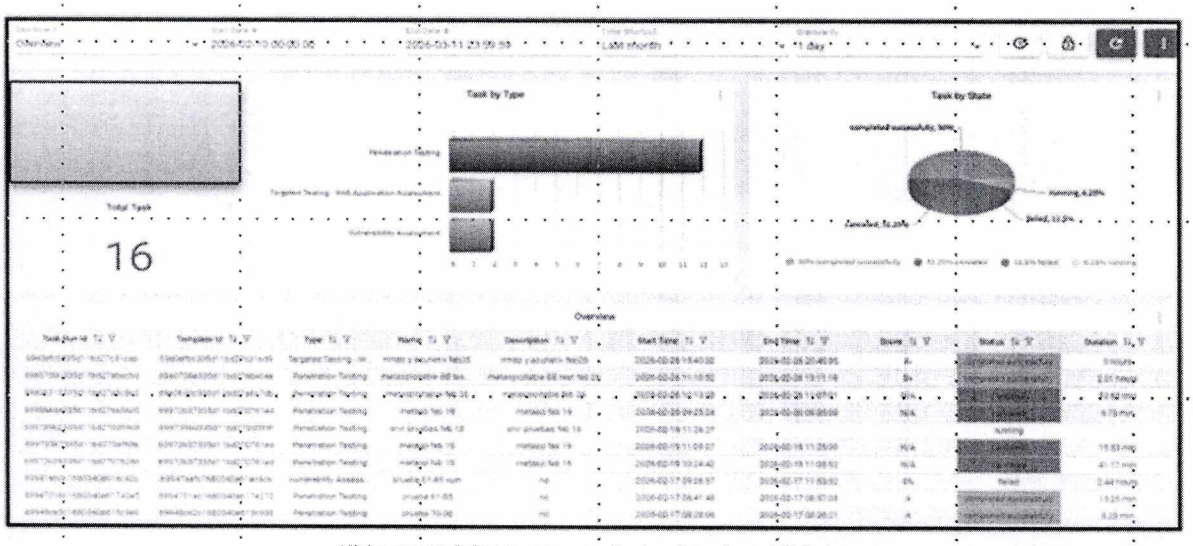
Describiendo la postura de seguridad de los activos observados a través de la distribución y priorización de riesgos identificados mediante herramientas tecnológicas como la de Enriquecimiento y contextualización de origen y Validación de seguridad

automatizada, enfocándose estrictamente en los segmentos que cuentan con una integración vigente al servicio de Observabilidad Avanzada.

Adicionalmente el servicio viene notificando sobre la estabilidad de la infraestructura bajo observación para supervisar la matriz de estrés y el estado de los activos críticos que están siendo monitoreados actualmente, permitiendo identificar degradaciones de rendimiento solo en aquellos componentes integrados al servicio de Observabilidad Avanzada hasta este momento.

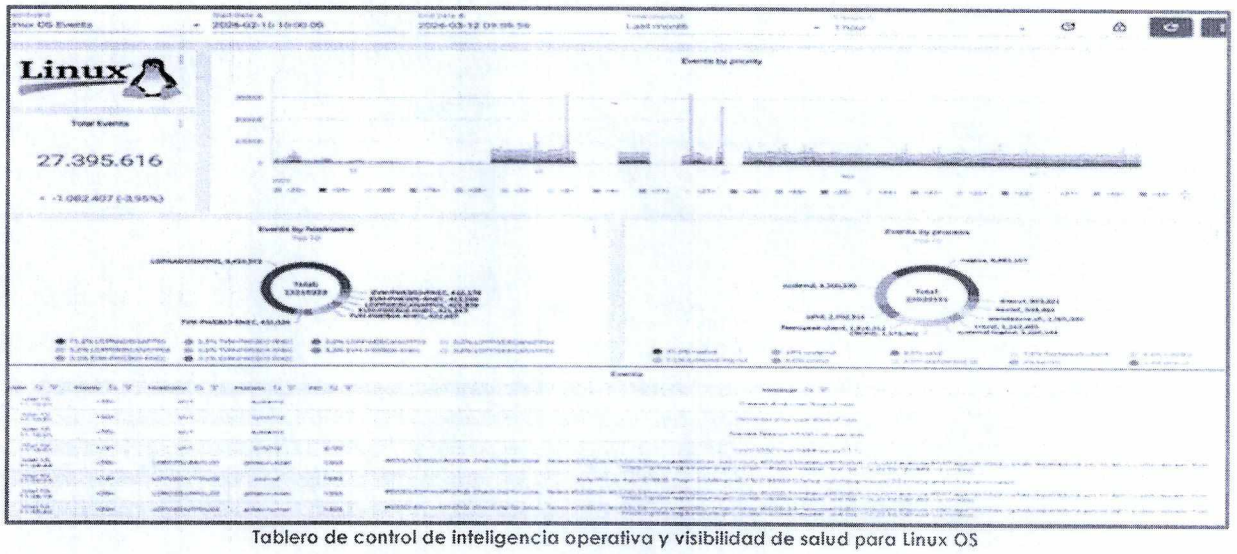
3.2 ACTIVIDADES REALIZADAS A NIVEL TÉCNICO

Se integraron los datos de autenticación y autorización con la visibilidad de las redes SD-WAN y SD-LAN. Esta consolidación permite centralizar el monitoreo de tráfico y acceso a recursos en el servicio de observabilidad avanzada, utilizando la información de las plataformas de red e identidad para supervisar integralmente los eventos en los segmentos vinculados.



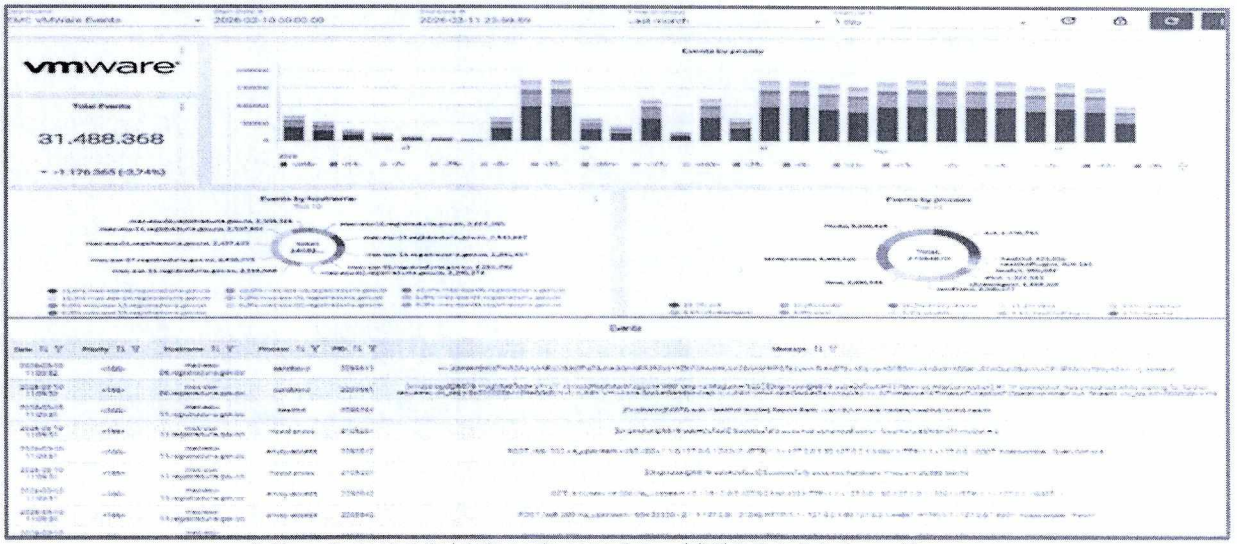
Vista general de tareas y resultados de vulnerabilidades

Durante el último mes, el panel de Pentera Core refleja una actividad operativa enfocada en la validación de seguridad con un total de 16 tareas ejecutadas, donde predomina el Penetration Testing con 12 sesiones frente a una menor frecuencia de escaneos de vulnerabilidades y pruebas web. Aunque el 50% de las actividades se completaron con éxito obteniendo calificaciones destacables de A y B+.



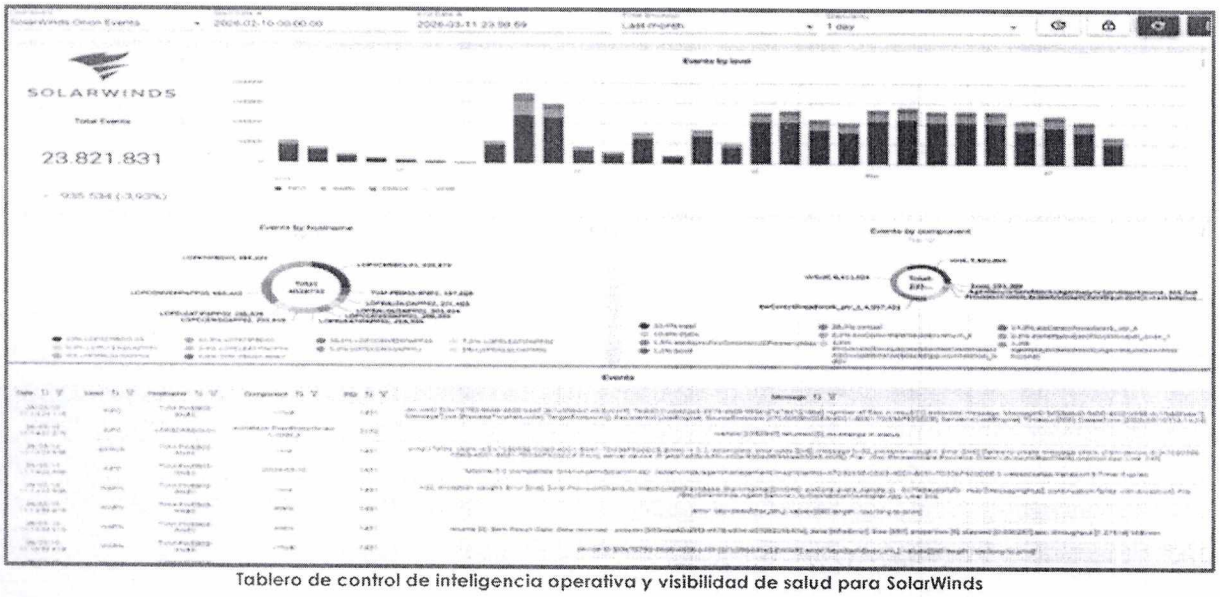
Tablero de control de inteligencia operativa y visibilidad de salud para Linux OS

El análisis descriptivo de los eventos de Linux en el último ciclo de monitoreo del 10 de febrero al 10 de marzo de 2026 revela un volumen total de 27.395.616 eventos, lo que representa una ligera disminución del 3,95% respecto al periodo anterior.



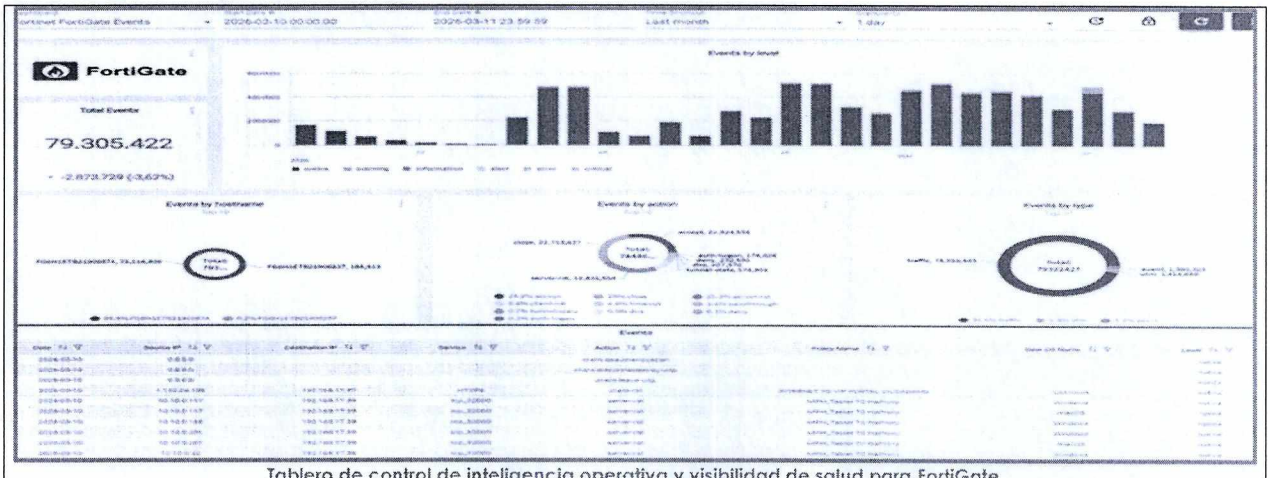
Tablero de control de inteligencia operativa y visibilidad de Salud para Vmware

El análisis de EMC VMware Events durante el último mes muestra un volumen de 31.488.368 eventos, lo que representa una ligera disminución del 3,74% respecto al periodo anterior. La actividad se concentra principalmente en el proceso sut, que genera el 23,3% de los registros 6,4 millones, seguido por Host con un 20,2%.



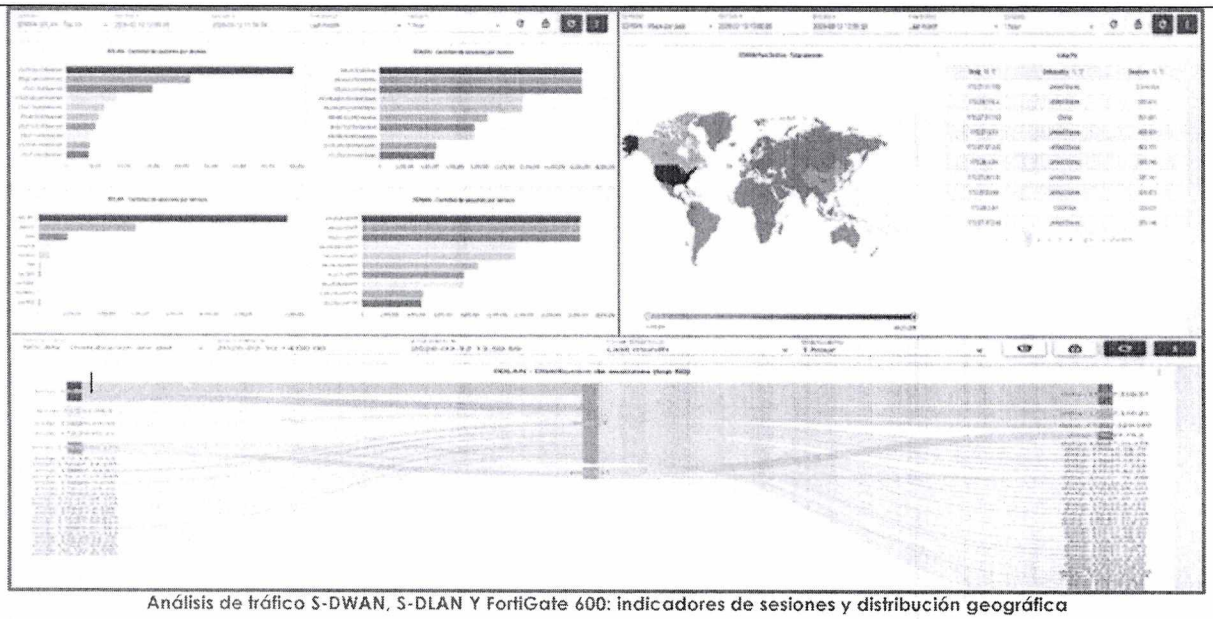
Tablero de control de inteligencia operativa y visibilidad de salud para SolarWinds

Basado en los tableros de control y registros de eventos de SolarWinds Orion, el último mes del 10 de febrero al 10 de marzo de 2026 muestra una actividad volumétrica significativa con un total de 23.821.831 eventos, a pesar de representar una ligera disminución del 3,93% respecto al periodo anterior. La distribución diaria revela picos de actividad alrededor del 19 de febrero y el 3 de marzo, donde el volumen de registros superó los 1,5 millones por día, predominando los niveles categorizados como INFO y WARN.



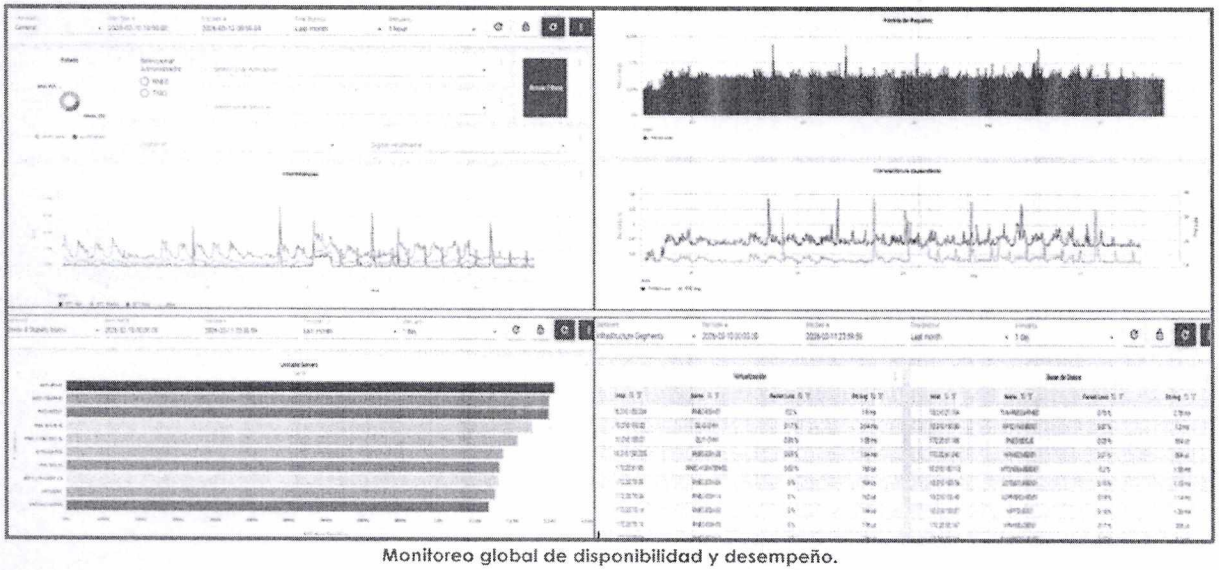
Tablero de control de inteligencia operativa y visibilidad de salud para FortiGate

En relación con el panel de eventos de Fortinet FortiGate, el último mes registró un volumen masivo de actividad con un total de 79.305.422 eventos, lo que representa una ligera disminución del 3,62% respecto al periodo anterior. La gran mayoría de estos registros corresponden a tráfico de red 96,5% y se clasifican casi en su totalidad bajo el nivel de severidad notice, con picos de actividad que superaron los 5 millones de eventos diarios hacia finales de febrero y principios de marzo. En cuanto a las acciones ejecutadas, existe una distribución equilibrada entre conexiones aceptadas 29,2%, cerradas 29% y reinicios del servidor o server-rst 25,3%, mientras que las denegaciones de tráfico representaron una fracción mínima del 0,3%.



Análisis de tráfico S-DWAN, S-DLAN Y FortiGate 600: indicadores de sesiones y distribución geográfica

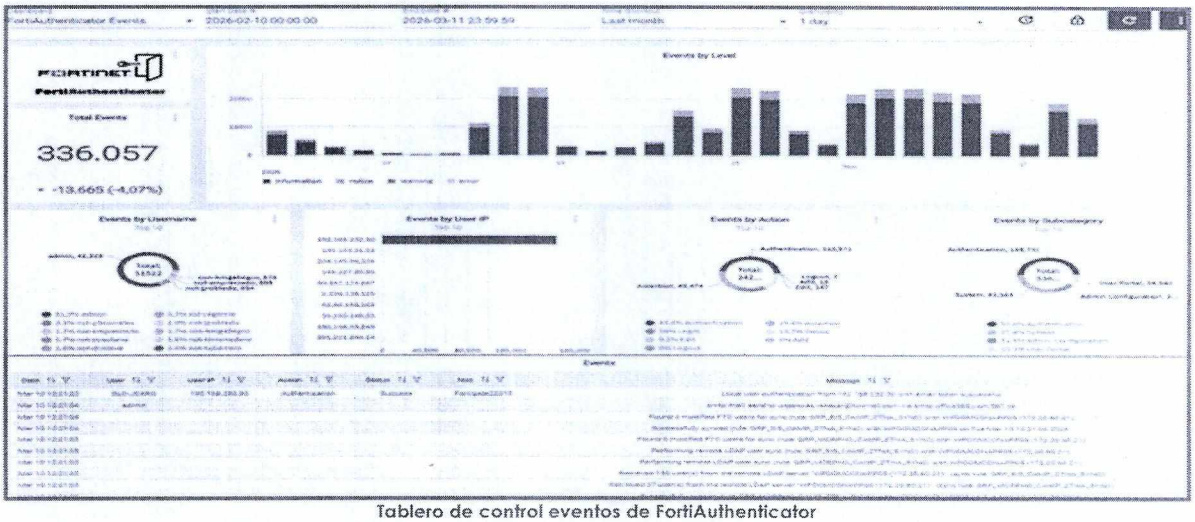
En el periodo analizado, el tráfico de red analizado muestra un volumen de actividad significativamente mayor en la infraestructura SDWAN en comparación con SDLAN, destacando una fuerte concentración de sesiones hacia destinos en Chile, Colombia y Estados Unidos.



Monitoreo global de disponibilidad y desempeño.

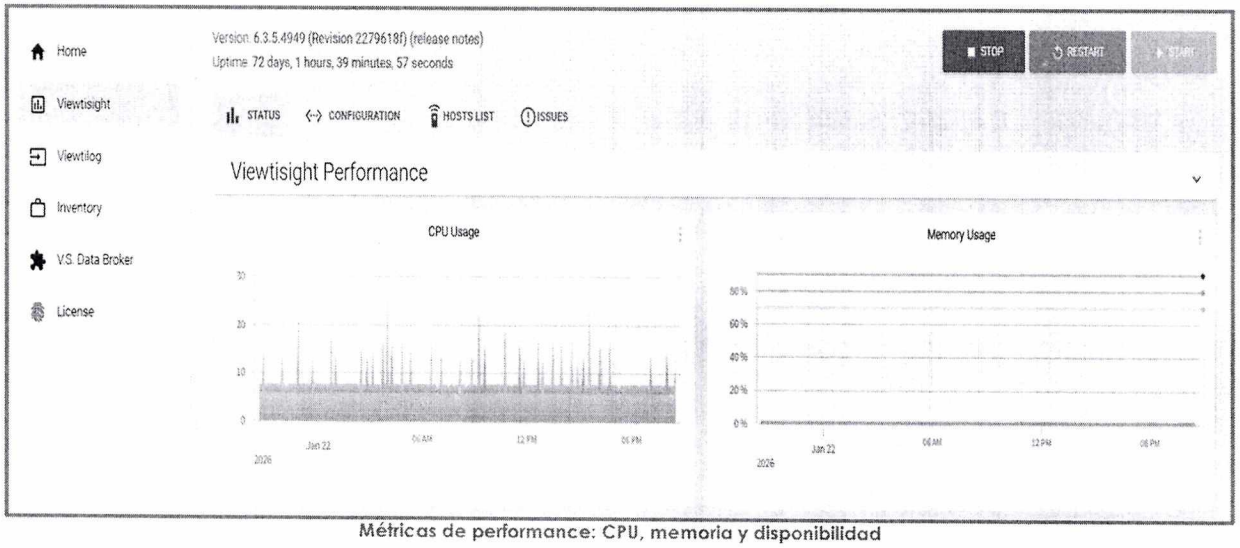
El análisis del último mes la pérdida de paquetes muestra una base constante cercana al 0,75%, con picos recurrentes que superan el 1,3%, este comportamiento se refleja directamente en la matriz de estabilidad.

En cuanto al desempeño por segmentos, la mayor concentración de registros se localiza en las aplicaciones de negocio, específicamente en los servicios de biometría, los cuales registran una pérdida de paquetes total del 100%. A nivel de latencia, el rol de controlador de dominio encabeza los tiempos de respuesta más altos, superando los 1,8 ms, mientras que servicios específicos como la página web y Onbase demandan la mayor atención técnica al promediar latencias cercanas a los 4 ms.



Tablero de control eventos de FortiAuthenticator

Durante el último mes, el sistema FortiAuthenticator registró un volumen total de 336.057 eventos, lo que representa una ligera disminución del 4,07% en comparación con el periodo anterior. La actividad estuvo dominada mayoritariamente por eventos de categoría "information", con picos de actividad que superaron los 20.000 registros diarios a finales de febrero y principios de marzo. En términos operativos, la subcategoría de "Authentication" fue la más relevante, abarcando el 50,5% del total de logs 169.731 eventos.



Métricas de performance: CPU, memoria y disponibilidad

Este tablero de control audita el rendimiento técnico de la plataforma mediante el monitoreo constante del procesador y la memoria RAM. Mientras que el gráfico de CPU refleja la carga generada por procesos pesados y visualizaciones, el consumo de memoria se mantiene bajo niveles seguros. Su objetivo principal es asegurar una experiencia de usuario ágil, permitiendo anticipar el escalado de infraestructura para evitar lentitud en la carga de datos.

3.3 ANÁLISIS DE RESULTADOS OBTENIDOS

El monitoreo del último periodo evidencia una ingesta continua y estable de telemetría a través de todas las capas de infraestructura integradas al modelo de observabilidad avanzada. Esta recolección centralizada de eventos provenientes de plataformas de red, sistemas operativos y herramientas específicas consolida una línea base técnica confiable para la operación diaria. Como parte natural del ciclo de madurez del servicio, el esfuerzo a corto plazo se orientará a la integración de fuentes priorizadas por la entidad, así como a la calibración gradual de las reglas de alertamiento sobre los tableros de control en producción, buscando afinar la identificación de patrones operativos sin alterar la continuidad de la visualización actual.

3.4 RECOMENDACIONES TÉCNICAS

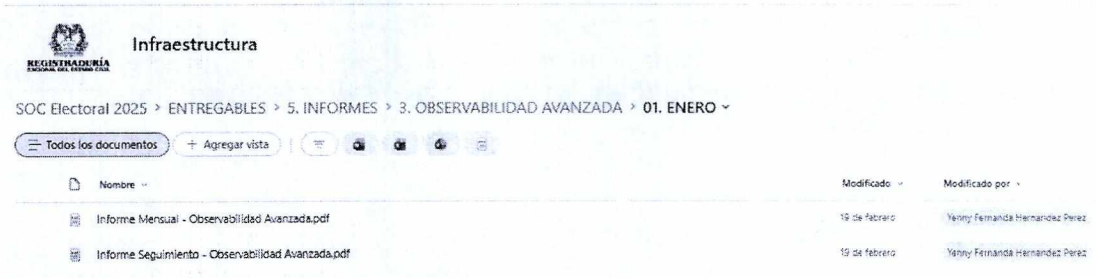
Mantener la continuidad con el proceso de integración de los componentes SD-LAN dentro del modelo de observabilidad avanzada, de manera que la telemetría de la infraestructura de red en las diferentes sedes se unifique con los estándares vigentes.

Se sugiere ejecutar simulaciones controladas de incidentes para garantizar que las reglas de correlación y los tableros de monitoreo mantengan su eficacia operativa tras cualquier actualización en la infraestructura.

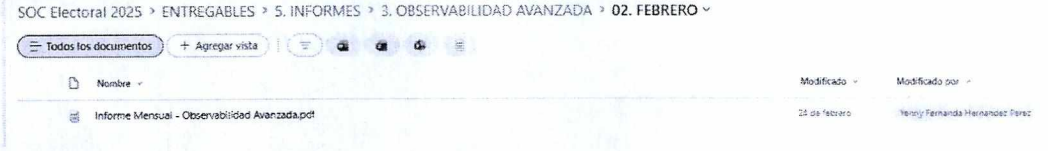
Es importante implementar un repositorio de control de versiones para respaldar configuraciones y conectores con el fin de garantizar la recuperación ante fallos y la consistencia técnica frente a futuras actualizaciones del sistema.

Durante este periodo se ha publicado los siguientes informes, los cuales se encuentran disponibles en la ruta dispuesta para el proyecto.

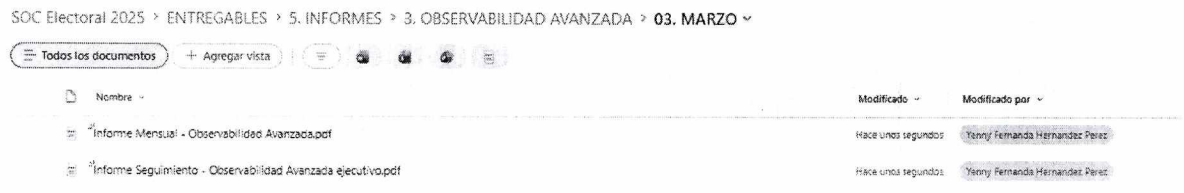
ENERO



FEBRERO



MARZO



4. SISTEMA INTEGRAL DE GESTIÓN DE RIESGOS Y CUMPLIMIENTO

4.1 RESUMEN DE LA OPERACIÓN CON LOS HALLAZGOS TÉCNICOS

Uno de sus pilares estratégicos es la implementación de un sistema integral de gestión de riesgos y cumplimiento, que proporcione una visión centralizada, correlacionada y en tiempo real del panorama de riesgos de ciberseguridad, facilitando la toma de decisiones informadas a nivel táctico y estratégico. Este componente automatiza los procesos de cumplimiento normativo, centraliza políticas y procedimientos, garantiza la trazabilidad y auditabilidad de las acciones, y mantiene un monitoreo continuo de activos críticos, contribuyendo a una gestión de seguridad más eficiente, medible y transparente.

A nivel del Pilar del Gestión del Riesgo, permite Identificar y detectar las vulnerabilidades presentes en la línea base configurada en la herramienta de escaneos, para la gestión del riesgo, la centralización, la priorización y el seguimiento de estas basadas en el riesgo.

4.2 ACTIVIDADES REALIZADAS A NIVEL TÉCNICO

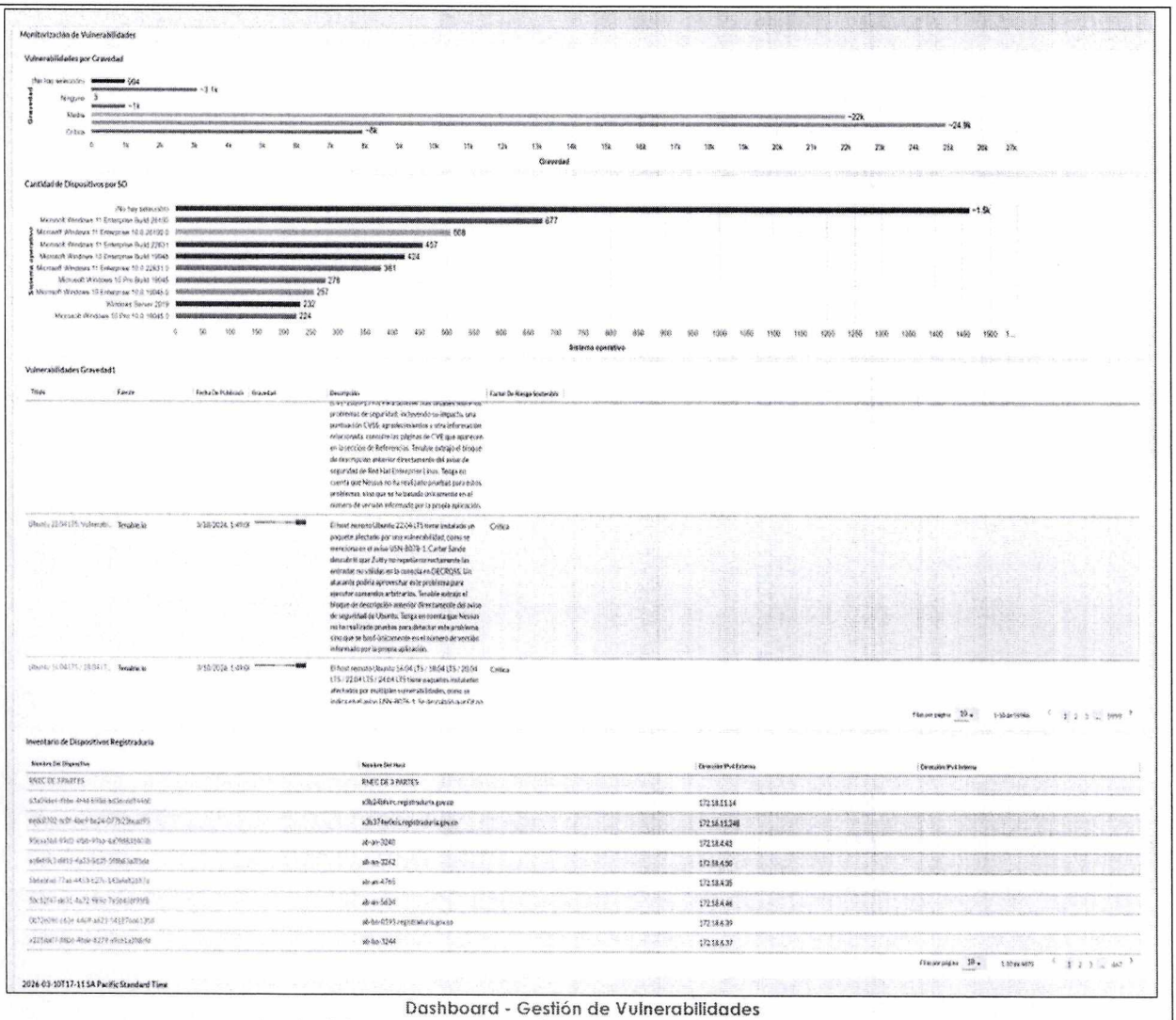
Gestión De Vulnerabilidades

o

El sistema integral GRC permitió realizar la integración con Tenable vía API-REST para transforma los datos técnicos de los escáneres en información de riesgo procesable para el negocio. El principal beneficio es que permite pasar de una larga lista de hallazgos técnicos a un proceso priorizado y automatizado que considera el contexto real del negocio. Dentro de la gestión del riesgo, las vulnerabilidades se pueden realizar las siguientes tareas:

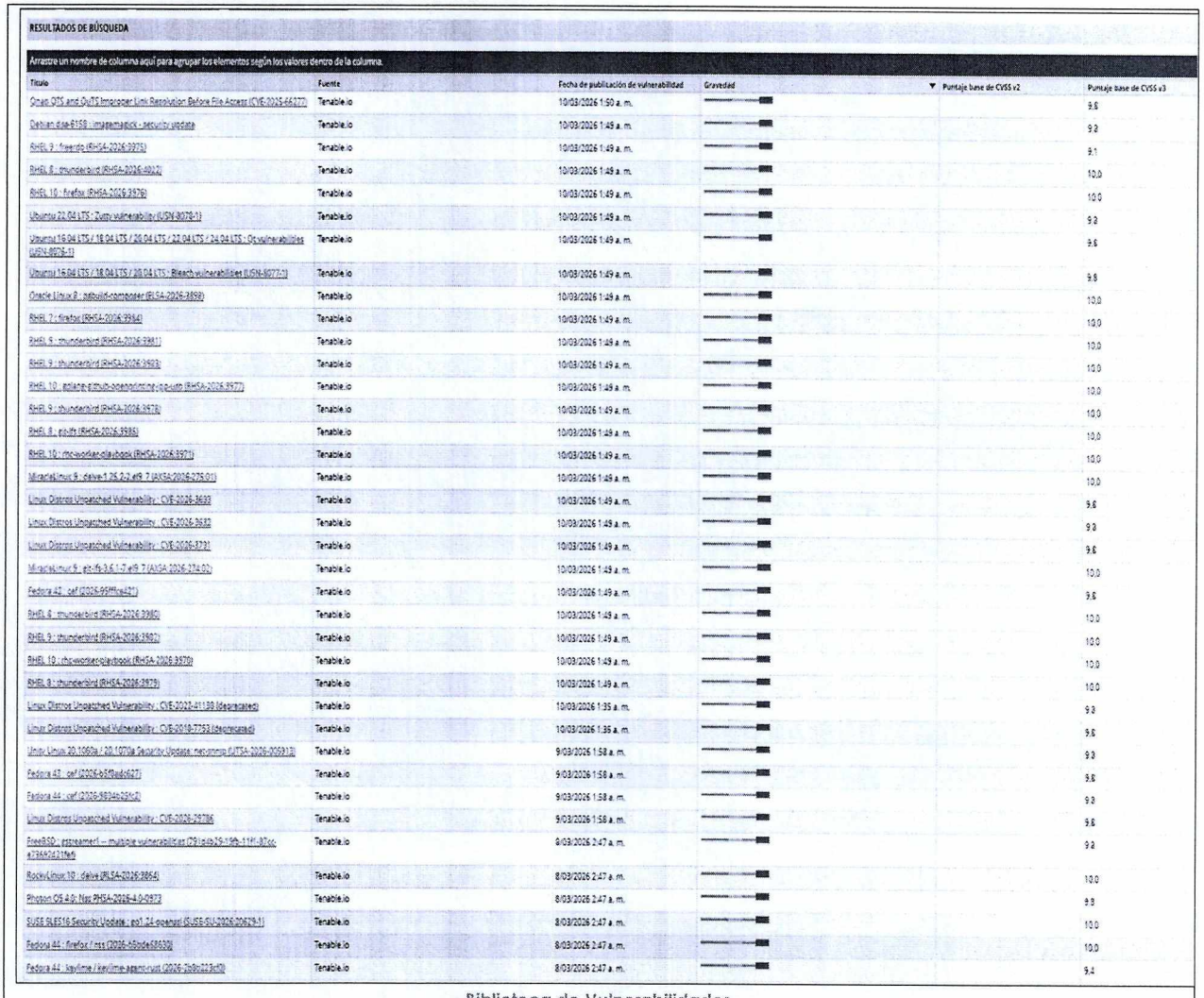
- Clasificar las vulnerabilidades según el nivel de severidad y criticidad del activo.
- Priorizar las vulnerabilidades para definir el plan de remediación.
- Identificar los activos críticos y de mayor exposición sobre la infraestructura tecnológica de la Registraduría Nacional del Estado Civil – RNEC para realizar el análisis de vulnerabilidades, clasificando éstas de acuerdo con la criticidad y explotabilidad.
- Generar el respectivo informe donde se describa la totalidad de las vulnerabilidades encontradas, clasificando por criticidad, explotabilidad y ubicación de éstas en la infraestructura tecnológica e informar a la Registraduría Nacional del Estado Civil – RNEC para que sean gestionadas.
- Realizar el respectivo seguimiento a los planes de remediación realizado por la Registraduría Nacional del Estado Civil – RNEC y verificar el estado de la infraestructura tecnológica con los planes desarrollados e implementados a través del seguimiento respectivo.

Esta herramienta centraliza todos los hallazgos de seguridad, permitiendo crear paneles de control y reportes ejecutivos en tiempo real. Esto facilita la toma de decisiones basada en datos y la comunicación del estado de la seguridad a la alta dirección.



Dashboard - Gestión de Vulnerabilidades
Fuente: Sistema Integral de Gestión de Riesgo – Gestión de Vulnerabilidades

La plataforma de Gobierno, Riesgo y Cumplimiento (GRC), aporta una capa de contexto y automatización que las herramientas de escaneo por sí solas no poseen. Esta herramienta permite visualizar en tiempo real las vulnerabilidades identificadas como se relaciona a continuación.



RESULTADOS DE BÚSQUEDA

Arrastre un nombre de columna aquí para agrupar los elementos según los valores dentro de la columna.

Título	Fuente	Fecha de publicación de vulnerabilidad	Gravedad	Puntaje base de CVSS v2	Puntaje base de CVSS v3
Qpid QTS and QuTS Improper Link Resolution Before File Access (CVE-2025-66277)	Tenable.io	10/03/2026 1:50 a. m.			9.8
Debian dsa-6158 : imagemagick - security update	Tenable.io	10/03/2026 1:49 a. m.			9.8
RHEL 9 : freerdp (RHSA-2026:3975)	Tenable.io	10/03/2026 1:49 a. m.			9.1
RHEL 8 : thunderbird (RHSA-2026:4002)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 10 : firefox (RHSA-2026:3979)	Tenable.io	10/03/2026 1:49 a. m.			10.0
Ubuntu 23.04 LTS : Zesty vulnerability (USN-8078-1)	Tenable.io	10/03/2026 1:49 a. m.			9.8
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Qs vulnerabilities (USN-8078-1)	Tenable.io	10/03/2026 1:49 a. m.			9.8
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Bleach vulnerabilities (USN-8077-1)	Tenable.io	10/03/2026 1:49 a. m.			9.8
Oracle Linux 8 : rebuild-composer (ELSA-2026-3898)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 7 : firefox (RHSA-2026:3984)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 9 : thunderbird (RHSA-2026:3981)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 9 : thunderbird (RHSA-2026:3983)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 10 : golang-github-openprinting-ipp-usb (RHSA-2026:3977)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 9 : thunderbird (RHSA-2026:3978)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 8 : go-rhn (RHSA-2026:3986)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 10 : rhc-worker-playbook (RHSA-2026:3971)	Tenable.io	10/03/2026 1:49 a. m.			10.0
MiraclaLinux 9 : delve-1.26.2-2.el9_7 (AXSA-2026-275-01)	Tenable.io	10/03/2026 1:49 a. m.			10.0
Linux Distros Unpatched Vulnerability : CVE-2026-3693	Tenable.io	10/03/2026 1:49 a. m.			9.8
Linux Distros Unpatched Vulnerability : CVE-2026-3692	Tenable.io	10/03/2026 1:49 a. m.			9.8
Linux Distros Unpatched Vulnerability : CVE-2026-3731	Tenable.io	10/03/2026 1:49 a. m.			9.8
MiraclaLinux 9 : go-fs-3.6.1-7.el9_7 (AXSA-2026-274-02)	Tenable.io	10/03/2026 1:49 a. m.			10.0
Fedora 42 : cef (2026-95ffe4d71)	Tenable.io	10/03/2026 1:49 a. m.			9.8
RHEL 8 : thunderbird (RHSA-2026:3980)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 9 : thunderbird (RHSA-2026:3982)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 10 : rhc-worker-playbook (RHSA-2026:3970)	Tenable.io	10/03/2026 1:49 a. m.			10.0
RHEL 9 : thunderbird (RHSA-2026:3976)	Tenable.io	10/03/2026 1:49 a. m.			10.0
Linux Distros Unpatched Vulnerability : CVE-2022-41190 (deprecated)	Tenable.io	10/03/2026 1:35 a. m.			9.8
Linux Distros Unpatched Vulnerability : CVE-2016-7753 (deprecated)	Tenable.io	10/03/2026 1:35 a. m.			9.8
Unity Linux 20.1060a / 20.1070a Security Update: nextcloud (UTSA-2026-000313)	Tenable.io	9/03/2026 1:58 a. m.			9.8
Fedora 43 : cef (2026-b59add627)	Tenable.io	9/03/2026 1:58 a. m.			9.8
Fedora 44 : cef (2026-9834b2d2c2)	Tenable.io	9/03/2026 1:58 a. m.			9.8
Linux Distros Unpatched Vulnerability : CVE-2026-26786	Tenable.io	9/03/2026 1:58 a. m.			9.8
FreeBSD : ntpsec#1 -- multiple vulnerabilities (791cb929-199b-11f1-87cc-e7669d231ef6)	Tenable.io	8/03/2026 2:47 a. m.			9.8
RockyLinux 10 : delve (RLSA-2026:3864)	Tenable.io	8/03/2026 2:47 a. m.			10.0
Photon OS 4.0: Nss PHSA-2026-4.0-0973	Tenable.io	8/03/2026 2:47 a. m.			9.8
SUSE SLES16 Security Update : go1.24-openssl (SUSE-SU-2026:20679-1)	Tenable.io	8/03/2026 2:47 a. m.			10.0
Fedora 44 : firefox / nss (2026-b5bde58600)	Tenable.io	8/03/2026 2:47 a. m.			10.0
Fedora 44 : keylime / keylime-agent-rust (2026-2b9c823cf0)	Tenable.io	8/03/2026 2:47 a. m.			9.4

Biblioteca de Vulnerabilidades
Fuente: Sistema Integral de Gestión de Riesgo – Gestión de Vulnerabilidades

Los "data feeds" de Archer consumen la API REST de Tenable.io para importar de manera automática y programada los activos descubiertos, los plugins y los resultados de vulnerabilidades. Al consolidar toda la información en Archer, se obtiene una visión completa que relaciona los activos críticos con sus vulnerabilidades reales.

Result

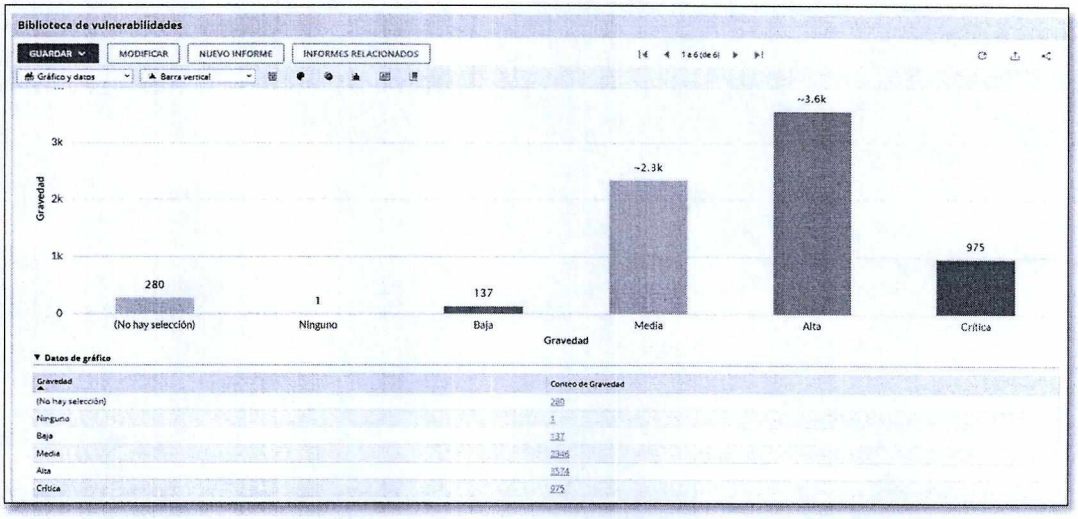
Manage Columns

Vulnerability Scan Result Title	Severity	VSR Overall Status	Impacted Device	Vulnerability Library Details
100025-445-TCP-e4ec221b0568405f94a21b04f0bab9fc	Not Started	Active	5d00c967-7f9c-440f-bae6-ca2cb7a38174	
100052-445-TCP-04a2552893be42b8bb29f3777c9258c	High	Active	af46b8bb-44fd-4581-99ea-2fedac516258	Adobe Flash Player <= 25.0.0.14 Multiple Vulnerabilities (APSB15)
100052-445-TCP-214a2d1f09dc4845adf6d7f1c71349f4	High	Active	e1882aaa-167d-431e-8821-af5389c3ce7f	Adobe Flash Player <= 25.0.0.14 Multiple Vulnerabilities (APSB15)
100052-445-TCP-238dbaa5f94b4740900a812f999d800	High	Active	9fea7a29-ab94-4a8c-90f8-68490acf545e	Adobe Flash Player <= 25.0.0.14 Multiple Vulnerabilities (APSB15)
100052-445-TCP-24e81191ba5e464ab20c30f1e335089	High	Active	5ff11e92-9422-4f4d-8d0a-e93d94104021	Adobe Flash Player <= 25.0.0.14 Multiple Vulnerabilities (APSB15)
100052-445-TCP-24fca14f834e4e6bacc427ad5213289e	High	Active	ecb331e0-72d5-4e9e-8671-c4d2b90b6043	Adobe Flash Player <= 25.0.0.14 Multiple Vulnerabilities (APSB15)
100052-445-TCP-2e4f172b67c841a4bf69589aa74e226	High	Active	6c808416-ba11-4d9a-aead-d64064ce8d4f	Adobe Flash Player <= 25.0.0.14 Multiple Vulnerabilities (APSB15)
100052-445-TCP-37b7f4488b9749ba9619fd3a71af018	High	Active	3c27b615-615e-46c8-a013-6616b2a255c2	Adobe Flash Player <= 25.0.0.14 Multiple Vulnerabilities (APSB15)
100052-445-TCP-41b66b512aed4765b37cd3d8ce7646c	High	Active	34aeb53b-b6a4-4943-8676-b3516ab1f82a	Adobe Flash Player <= 25.0.0.14 Multiple Vulnerabilities (APSB15)
100052-445-TCP-446d5048be2d4b56af8e384e1136e21	High	Active	afd56031-44bf-478e-8cd4-b4f1a0fafe07	Adobe Flash Player <= 25.0.0.14 Multiple Vulnerabilities (APSB15)
100052-445-TCP-47ee633ce7584bf6a5e69cee5d917d5	High	Active	7e068c6d-a65b-412c-b589-3953e64983bb	Adobe Flash Player <= 25.0.0.14 Multiple Vulnerabilities (APSB15)

Resultados de Escaneos.
Fuente: Sistema Integral de Gestión de Riesgo – Vulnerabilidades

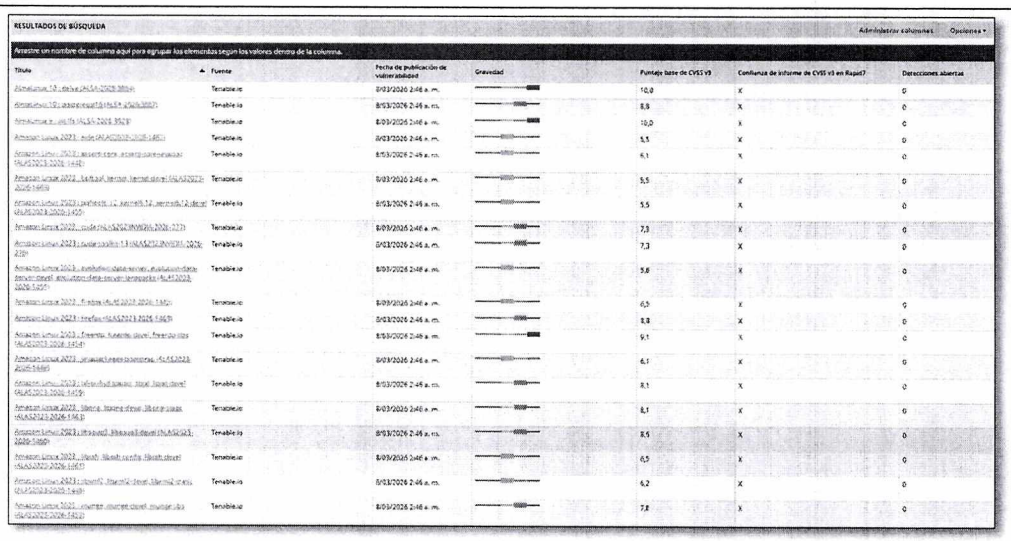
4.3 ANÁLISIS DE RESULTADOS OBTENIDOS

De acuerdo con el análisis de escaneo de Vulnerabilidades durante el periodo, se tiene la siguiente gráfica de escaneos de Vulnerabilidades:



Sistema Integral de Gestión de Riesgo – Vulnerabilidades

De acuerdo a la información suministrada por el servicio del sistema integral GRC, se evidencia que en el último mes se han escaneado 7313 vulnerabilidades en total, donde las Vulnerabilidades altas, son las que tienen mayor porcentaje de 48,87%; el cual representa la mayor porcentaje casi la mitad, esto representa una posible materialización de amenazas para la seguridad de la entidad, las vulnerabilidades medias se presentan en un porcentaje de 32.08% , donde se suman con las altas y dan un peso del 80% de las vulnerabilidades, el cual es un impacto elevado, teniendo en cuenta que la exposición es alta y no se ha efectuado una remediación efectiva, y continúan las críticas con un porcentaje de 13,33%; Por lo anterior se presenta la amenaza alta de probabilidad de explotación. Se relaciona a continuación las vulnerabilidades del mes de marzo de 2026 identificadas en el sistema Integral de Gestión de Riesgo – Vulnerabilidades.



Sistema Integral de Gestión de Riesgo – Vulnerabilidades

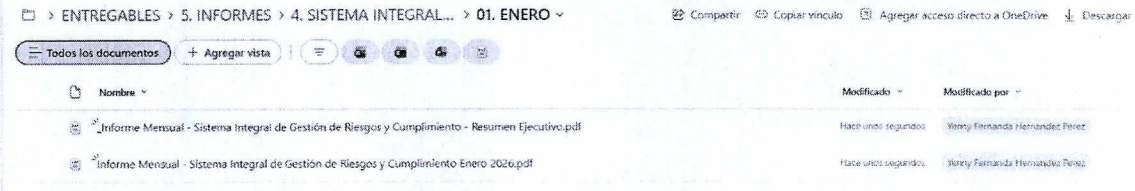
4.4 RECOMENDACIONES TÉCNICAS

Mediante la gestión de Vulnerabilidades se realizan las siguientes recomendaciones:

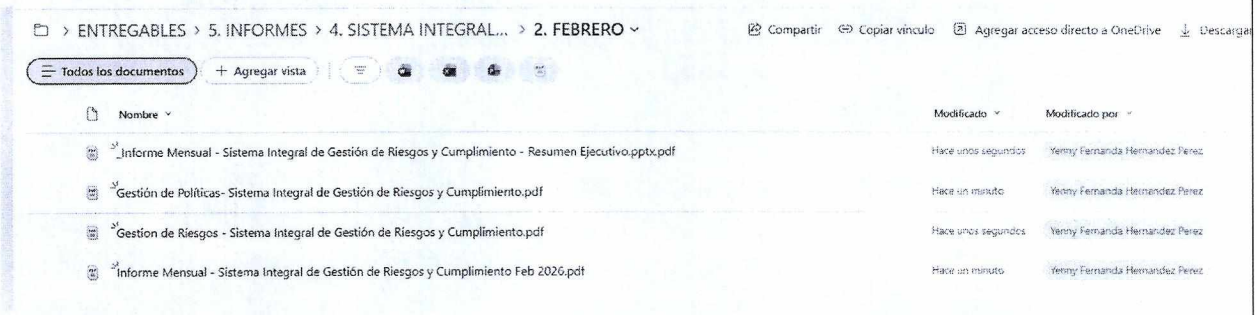
- Realizar planes de mejora en cuanto a medidas de mitigación y remediación de vulnerabilidades.
- Acorde con los resultados del último mes es necesario realizar una remediación prioritaria.
- Realizar planes de remediación para reducir el riesgo de explotación de las vulnerabilidades con priorización de acuerdo con la gravedad.
- Realizar las respectivas recomendaciones a la Registraduría Nacional del Estado Civil – RNEC sobre la aplicabilidad o no de los planes de remediación en la infraestructura tecnológica y los posibles escenarios que se pueden llegar a presentar en caso de no tomar en cuenta o llevar a cabo las remediaciones necesarias.

Durante este periodo se ha publicado los siguientes informes, los cuales se encuentran disponibles en la ruta dispuesta para el proyecto.

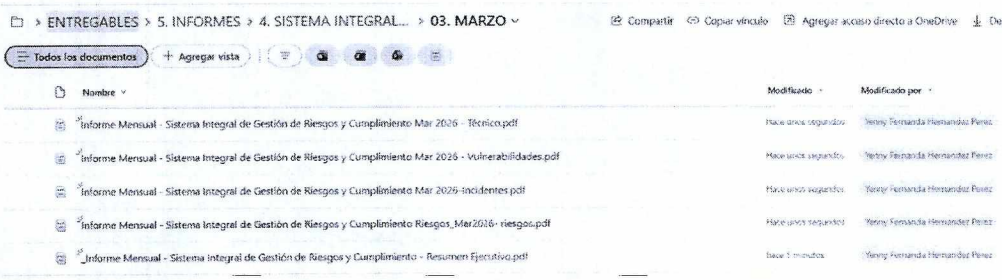
ENERO



FEBRERO



MARZO



Es importante resaltar que la auditoría realizada a los sistemas relacionados representa únicamente una fotografía del estado del proyecto en el momento de la evaluación. A medida que la plataforma evoluciona y se integran nuevos componentes o funcionalidades, podrían emerger vulnerabilidades adicionales, incluso de mayor criticidad.

Por esta razón, resulta indispensable establecer un proceso continuo de gestión de seguridad y auditorías periódicas que permitan anticipar riesgos, fortalecer los controles implementados y mantener la protección del portal frente a escenarios de amenaza en constante cambio.

En cumplimiento de cada una de las obligaciones del Contratista, la ejecución y seguimiento por parte de la supervisión del contrato de prestación de servicios del contrato No. 068 de 2025, se desarrolló conforme a lo establecido en el Anexo Técnico y la CLÁUSULA TERCERA del Contrato, mediante la cual se estableció para el cuarto pago.

En este Informe de actividades No.4, se describieron los componentes entregados que conforman el pago No. 04.

En esta cuarta revisión, se evidencia cumplimento por parte del proveedor de manera satisfactoria con los términos y condiciones establecidos en el acuerdo técnico y las actividades de Servicios para implementar la Ciberseguridad y Seguridad de la información para la organización y realización de los procesos electorales a llevarse a cabo en las vigencias 2025 y 2026.

De acuerdo con lo anterior, la supervisión del contrato confirma que el contratista cumple con los requerimientos establecidos en el Contrato 068 de 2025.

Así mismo, se adjunta CD con evidencias de las actividades expuestas en el informe.

Que el Contratista acreditó en debida forma, el cabal cumplimiento de las obligaciones relativas al Sistema de Seguridad Social Integral, atendiendo a lo establecido en el artículo 50 de la Ley 789 de 2002.

Asegurando el despliegue eficiente y puntual de los servicios acordados; a continuación, se describen los numerales supervisados:

BALANCE FINANCIERO:

CONTRATO 068 DE 2025 – UNE	
VALOR DEL CONTRATO	**$ 41.129.839.384**
Primer Pago: Fase de Planificación y alistamiento: Cronograma, planificación de actividades, hitos y fechas críticas para cada componente. Presentación del equipo de trabajo; matriz de riesgos, entrega de suscripciones.	**$ 314.946.326**
Segundo pago: Implementación de la prestación del servicio: Activación y entrega de los pilares con la ejecución de las siguientes actividades: A. Enriquecimiento y contextualización de origen; Visualización de un mapa dinámico de amenazas globales, Puntuación de riesgos por fuente maliciosa detectada, ificación de actividades, hitos y fechas críticas para cada componente. Presentación del equipo de trabajo; matriz de riesgos, entrega de suscripciones. B. Validación de seguridad automatizada	**$ 7.165.800.743**
Tercer Pago: Implementación de la prestación del servicio: Activación y entrega de los pilares con la ejecución de A. Observabilidad Avanzada. B.Sistema Integral de Gestión y Riesgo y Cumplimiento. C. Informe Operativo1.	**$ 4.777.198.470**
Cuarto Pago: Implementación de la prestación del servicio: Activación y entrega de los pilares con la ejecución de A. Observabilidad Avanzada. B.Sistema Integral de Gestión y Riesgo y Cumplimiento. C. Informe Operativo2.	**$ 8.523.111.492**
SALDO	**$ 20.348.782.353**

En constancia de lo anterior, se firma el presente informe, a los diecies (16) días del mes de marzo de 2026.

SUPERVISOR

HOSLANDER ADLAI SÁENZ BARRERA
Gerente de Informática

Proyectó: JUAN ALBERTO CARDONA MOLINA
Revisó: EDUARDO EMILIO CALDERÓN NARVAEZ