

 REGISTRADURÍA NACIONAL DEL ESTADO CIVIL	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0
CONTRATO:	Aprobado: 06/06/2017 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.	2			
PERIODO DE EJECUCIÓN:	1 de noviembre al 30 de noviembre 2025			
FECHA PRESENTE INFORME:	17 de diciembre de 2025			

 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

INFORME DE ACTIVIDADES CORRESPONDIENTES AL PAGO NO. 2.

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 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. 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.

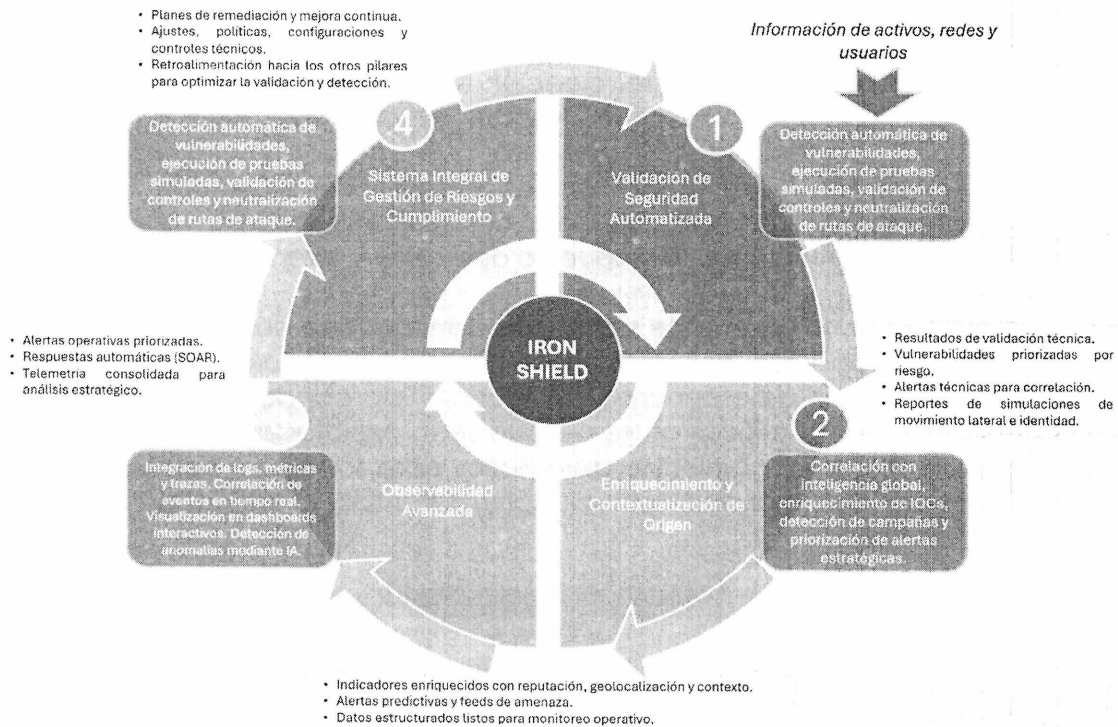
Este servicio se concibe como una arquitectura funcional que se integra y fortalece los procesos y procedimientos establecidos en Centro de Operaciones de Seguridad (SOC) actual, soportada en cuatro pilares estratégicos, cuya operación será articulada

	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORIA	VERSIÓN	0

Aprobado:
06/06/2017

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.

 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

EVOLUCIÓN DEL SERVICIO / AVANCES



REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL



Enriquecimiento y Contextualización De Origen

- Se habilitó el módulo de consultas de fuentes maliciosas.
- Se realizaron verificaciones de las IP's sospechosas para los eventos electorales de Consejos de Juventud 2025 y la Consulta Partidos 2025.
- Se validan en tiempo real los indicadores de compromiso presentes en la operación SOC.

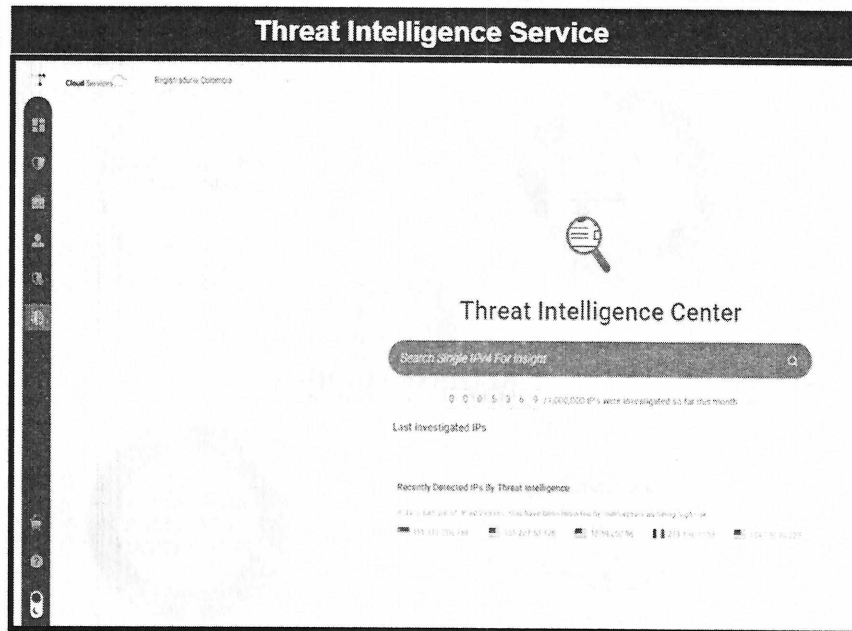
Validación de Seguridad Automatizada

- Durante el periodo evaluado se han realizado 14 actividades de identificación de vulnerabilidades de servicios asociado al proceso electoral, entregando las pruebas realizadas identificando falencias de XSS, SQLi, LFI, y RFI Y Credenciales filtradas.

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

Aprobado:
06/06/2017

1. ENRIQUECIMIENTO Y CONTEXTUALIZACIÓN DE ORIGEN



Gráfica: Portal Threat Intelligence Service. Fuente: Threat Intelligence Service.

Solución Implementada

Se pone en producción el portal de Threat Intelligence que permite dotar al SOC de visibilidad inmediata sobre fuentes maliciosas, reducir el Tiempo Medio de Resolución (MTTR).

Se utiliza en los eventos electorales de Consejos de Juventud 2025 y en la Consulta Partidos 2025.

El servicio se encuentra disponible 24 horas 7 días a la semana 365 días al año.

La inteligencia se aplica directamente en los centros de mitigación del fabricante.

Se habilitó el módulo de consultas de fuentes maliciosas.

Se habilita la conexión segura con el Threat Intelligence Cloud mediante actualizaciones automáticas de firmas e IPs maliciosas.

	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado:
06/06/2017

Permite realizar un Millón (1.000.000) de consultas cada mes; a la fecha del corte se realizaron aproximadamente 5369 consultas.



Suscripción y aprovisionamiento

Se habilitó el módulo de consultas de fuentes maliciosas.

Esta herramienta se utilizó en las elecciones de Consejos de Juventud 2025, en la Consulta Partidos 2025 y elecciones alcaldía de Villeta.

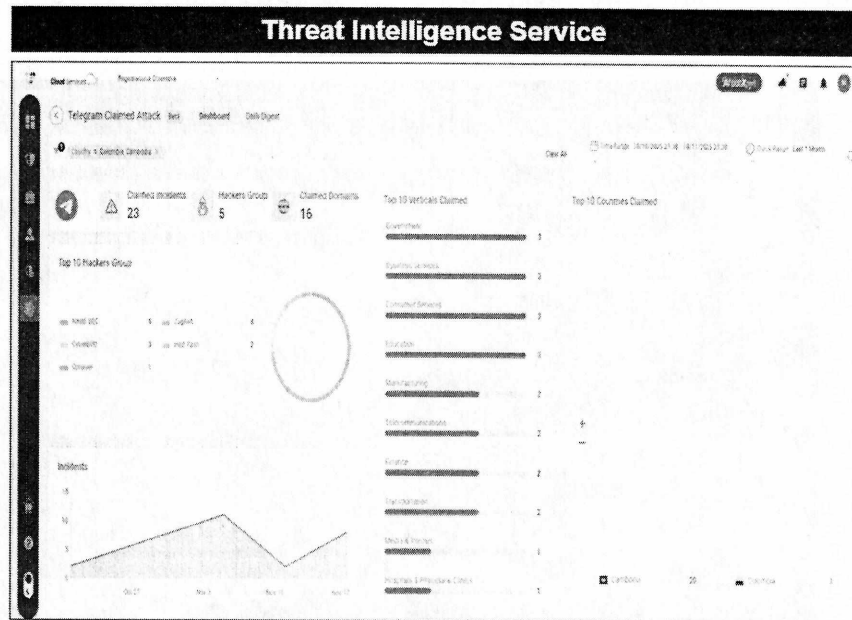
Visualización Global

La solución permite la transformación de datos sin procesar en información contextualizada, incluyendo eventos relacionados con ataques DDoS, actividad de bots y eventos asociados a políticas WAF, donde, obtiene su información a partir de una red global de interceptores de atacantes de DDoS, WAF, API y bots, con capacidad de análisis de tráfico web y de red capturado en producción.

Este permite acceso directo a través de un portal en la nube, el cual debe incluir un módulo de inteligencia reputacional que permita visualizar insights sobre las direcciones IP consultadas.

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

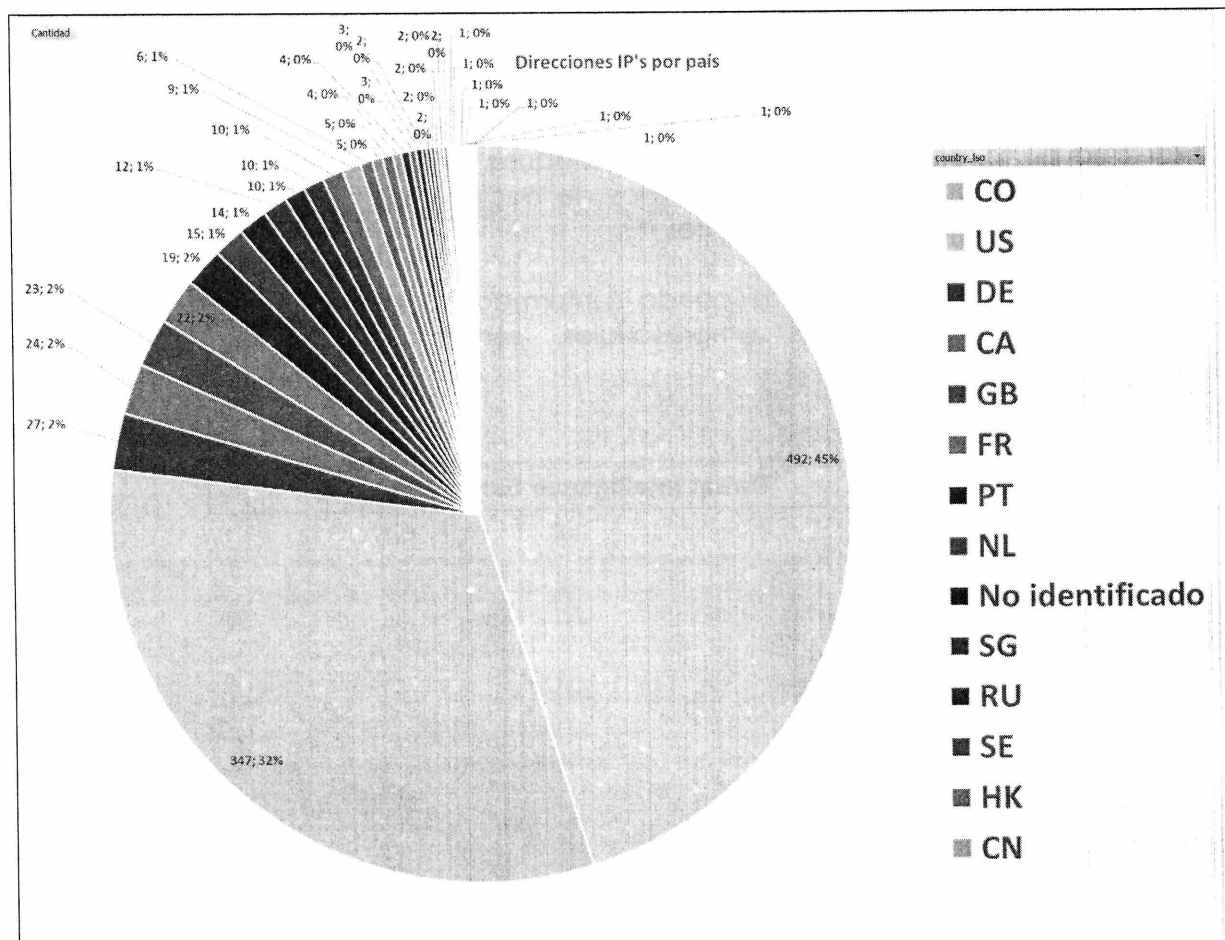
Aprobado:
06/06/2017



Gráfica: Portal Threat Intelligence Service. Fuente: Threat Intelligence Service - Contextualización de Entorno.

 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



Grafica global: En la gráfica se puede observar los países de origen de las direcciones IPs analizadas durante el periodo del 17 al 31 de octubre de 2025.

Evaluación Fuentes abiertas

Este pilar permite crear las bases para una respuesta informada, basada en contexto y alineada con las dinámicas reales del entorno de amenazas.

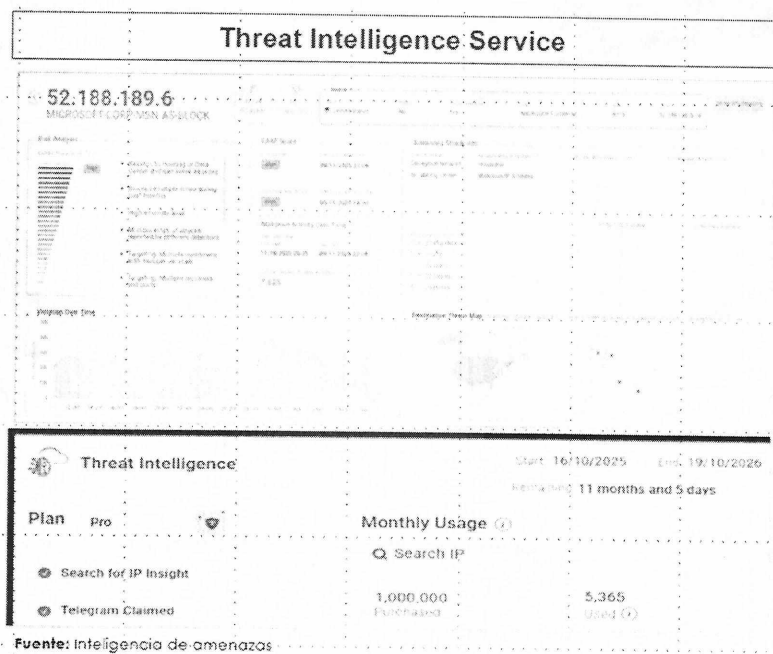
 REGISTRADURÍA NACIONAL DEL ESTADO CIVIL	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado:
06/06/2017

La herramienta realiza la recolección y análisis de información pública proveniente de redes sociales, registros y feeds comerciales para aportar contexto adicional a cada incidente.

Por otra parte, se generan reportes de ataques reivindicados en fuentes abiertas, mostrando reclamos públicos de grupos de hacking, con actualización constantes para detectar amenazas emergentes.

La herramienta crea un top clasificando la información clasificándolo en criterios como gubernamentales, servicios empresariales, servicio al cliente; educación y manufactura.



En estas elecciones, se realizó el análisis de las Ip's relacionadas, las cuales permiten que una búsqueda repetida de una misma IP no sea contabilizada como una nueva consulta.

Provee acceso directo a través de un portal en la nube, el cual debe incluye inteligencia reputacional que visualiza insights sobre las direcciones IP consultadas.

 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



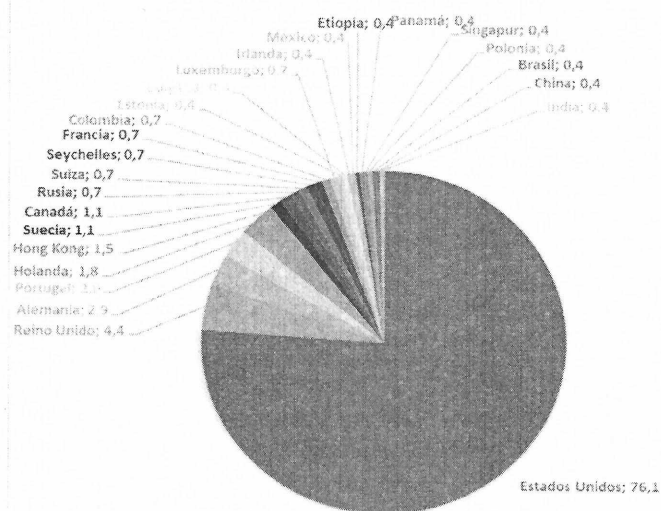
Gráfica: Indicadores de Compromiso. **Fuente:** Threat Intelligence Service. Ej. Estado de IP - 147[.]135[.]15[.]16.

Se hace entrega de primer informe de 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 interno (como comunicaciones a servidores de Comando y Control o exfiltración de datos), permitiendo 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.

 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



Gráfica. Fuentes de direcciones IP's por país (242 ip's) – Fuente: Threat Intelligence Service

De acuerdo con la validación de 242 IP's evaluadas, se evidencia una alta concentración en Estados Unidos, que representa el 76.1% del total.

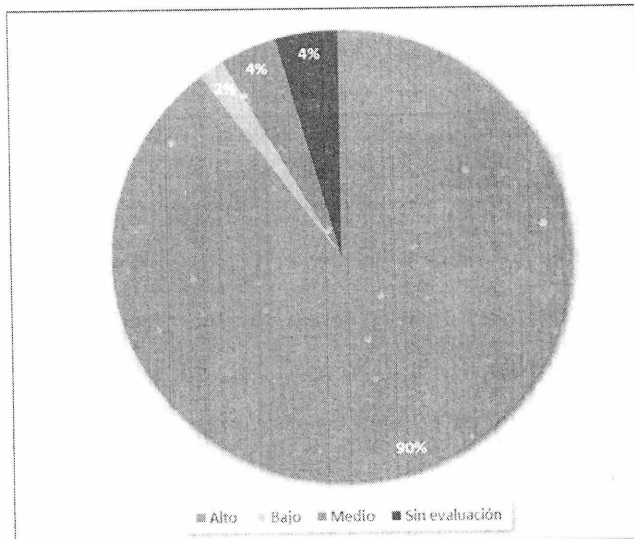
El otro gran porcentaje es de Europa, seguido de Asia, finalizando con América sin tener en cuenta Estado Unidos. Colombia representa menos del 1% en cuanto al origen de las amenazas.

Esta concentración puede reflejar tanto la cantidad de recursos tecnológicos en Estados Unidos, como el uso de servicios globales o mecanismos de ocultamiento (VPN, proxys) ubicados en dicho país.

Se identificó un alto volumen de conexiones y eventos relacionados con direcciones IP catalogadas como maliciosas o sospechosas, con una concentración significativa en Estados Unidos (76.1% del total). Esto refleja que gran parte de la actividad de amenaza global se origina o transita por infraestructuras en ese país, lo que implica que la defensa debe priorizar inteligencia específica sobre esas direcciones IP's.

	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado:
06/06/2017



Gráfica. Elecciones Alcalde Villeta – Fuente: Threat Intelligence Service - Clasificación de riesgo de direcciones IP's (242).

Para las elecciones del alcalde de Villeta 2025, se evidencia que la criticidad de las direcciones IP evaluadas indica que el 90% son de alto riesgo, subrayando la importancia de atender prioritariamente estos vectores de ataque para proteger la infraestructura tecnológica de la entidad.

El tráfico entrante detectado representa intentos activos de intrusión, escaneo o explotación. El tráfico saliente muestra posibles compromisos internos que podrían estar comunicándose con infraestructuras de comando y control o realizando exfiltración de datos.

Lo anterior requiere una vigilancia activa y respuesta rápida para minimizar impactos.

La inteligencia de amenazas y el análisis forense aplicado permitieron atribuir la actividad detectada a tácticas, técnicas y procedimientos (TTPs) específicos de actores maliciosos, lo cual es vital para mejorar la efectividad en la respuesta a incidentes y fortalecer las defensas.

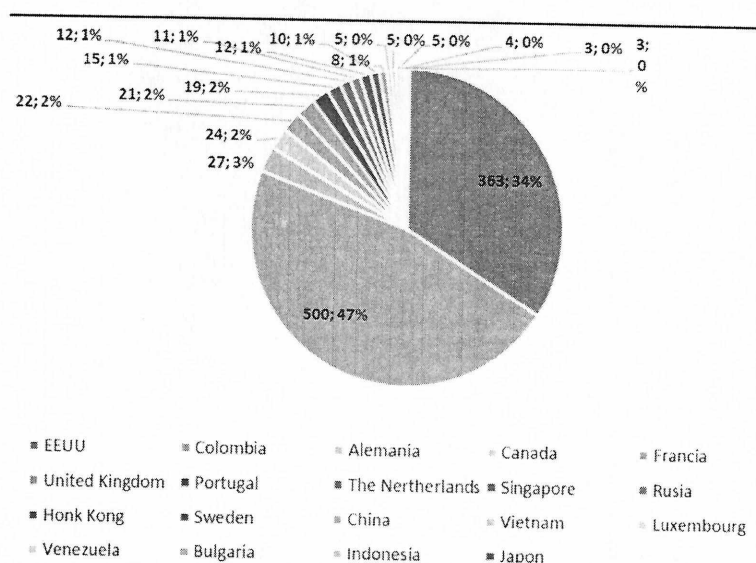
De acuerdo con el monitoreo en tiempo real se muestra cuáles son los puertos más escaneados, son los más usados como se muestra en la imagen de la derecha.

En estos puertos se han identificado vulnerabilidades los cuales han sido reportadas.

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

Aprobado:
06/06/2017

Enriquecimiento y Contextualización de Origen



Gráfica. Fuentes de direcciones IP's por país (1101 IP's) - Fuente: Threat Intelligence Service

El análisis de reputación de IP's concluye que el 44% de las direcciones evaluadas lo que equivale a 485 representan una criticidad alta.

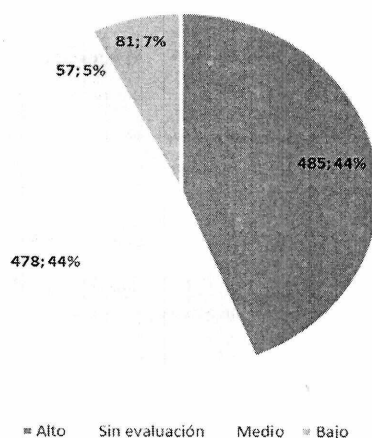
Esta clasificación se debe a que son amenazas confirmadas y actualmente activas, habiendo ejecutado acciones maliciosas recientemente.

Colombia representa menos del 1% en cuanto al origen de las amenazas.

Su criticidad se debe a que estas IP's han sido reportadas y validadas por múltiples fuentes de inteligencia de amenazas. Además, demuestran una alta versatilidad, ya que se ha confirmado su participación en diversos tipos de ataques, como la Denegación de Servicio (DoS), y operan a través de múltiples puertos y protocolos. Esta capacidad de adaptar sus vectores de ataque las convierte en una amenaza latente y versátil para la organización.

 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



Gráfica: Clasificación de riesgo de direcciones IP's (1101 IP's) -
Fuente: Threat Intelligence Service.

Su criticidad se debe a que estas IP's han sido reportadas y validadas por múltiples fuentes de inteligencia de amenazas. Además, demuestran una alta versatilidad, ya que se ha confirmado su participación en diversos tipos de ataques, como la Denegación de Servicio (DoS), y operan a través de múltiples puertos y protocolos.

Esta capacidad de adaptar sus vectores de ataque las convierte en una amenaza latente y versátil para la organización.

 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



2. VALIDACIÓN DE SEGURIDAD AUTOMATIZADA

La solución de Seguridad Automatizada permite realizar:

- Simulación de forma automática y continua ataques reales (incluyendo vectores de ataque complejos y cadenas de ataque) en todas las capas de ciberseguridad.
- Identifica brechas y debilidades en la infraestructura de seguridad.
- Funciona sin necesidad de instalar agentes en los activos a probar.

Identificación de Riesgos Reales:

- Se enfoca en vulnerabilidades explotables, malas configuraciones, credenciales filtradas y privilegios excesivos, resolviendo el problema de los altos "falsos positivos".
- Utiliza un motor de ataque algorítmico para generar y probar miles de vectores de ataque.

	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado:
06/06/2017



La solución de seguridad Automatizada,

- Examina la superficie de ataque externa (Pentra Surface) mapeando continuamente los activos orientados a la web.
- Ofrece capacidades para entornos nativos en la nube (Pentra Cloud), validando configuraciones, permisos y secretos expuestos.
- Valida la seguridad de la red interna.

Reporte y Remediación Guiada:

- Genera informes instantáneos y detallados al final de cada prueba.
- Prioriza las vulnerabilidades explotables basándose en su impacto real en la organización.
- Proporciona un plan de acción paso a paso para eliminar las exposiciones de manera efectiva.

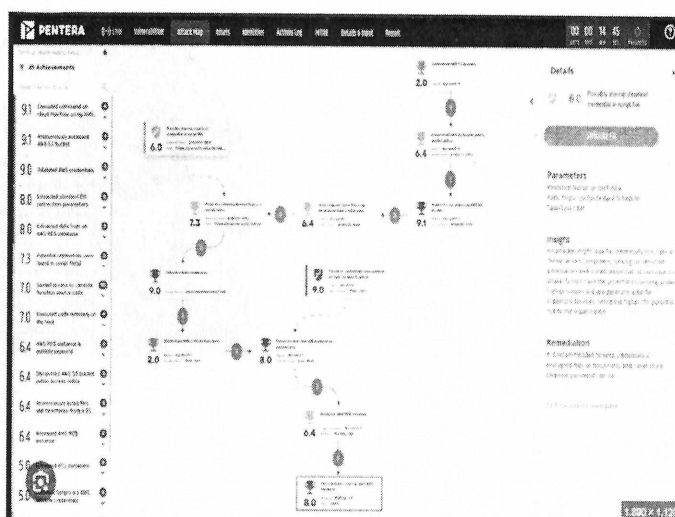
Seguridad y Flexibilidad:

- Opera de manera segura, sin comprometer la disponibilidad de los servidores.

 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

- Permite ajustar la intensidad del test, desde modos silenciosos hasta ataques más "ruidosos".
-
- Ofrece opciones para programar la repetición de los tests o ejecutarlos al instante.



La solución de seguridad Automatizada permite:

- Realizar pruebas automatizadas para hasta 3.000 activos.
- Descubrir automáticamente de activos externos a través de metodología OSINT.
- Usar protocolos de Capa 3 para detectar recursos sin credenciales y movimientos laterales.

DESPLIEGUE DETALLADO

Para el despliegue, se cuenta con el servidor Ubuntu Ver. 22.04 instalado como base, en la dirección IP 172.20.91.115, donde se ha desplegado la herramienta con acompañamiento del fabricante en la URL.

De acuerdo con el cronograma propuesto se han cumplido las siguientes tareas:

	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado:
06/06/2017

- Creación de usuarios.
- Registro de direcciones y URL de pruebas.
- Personalización de reportes.
- Creación de datos para la integración con herramienta Viewtinnet.
- Puesta en marcha y pruebas iniciales.
- Reportes detallados, ejecutivo.
- Evaluación de credenciales filtradas



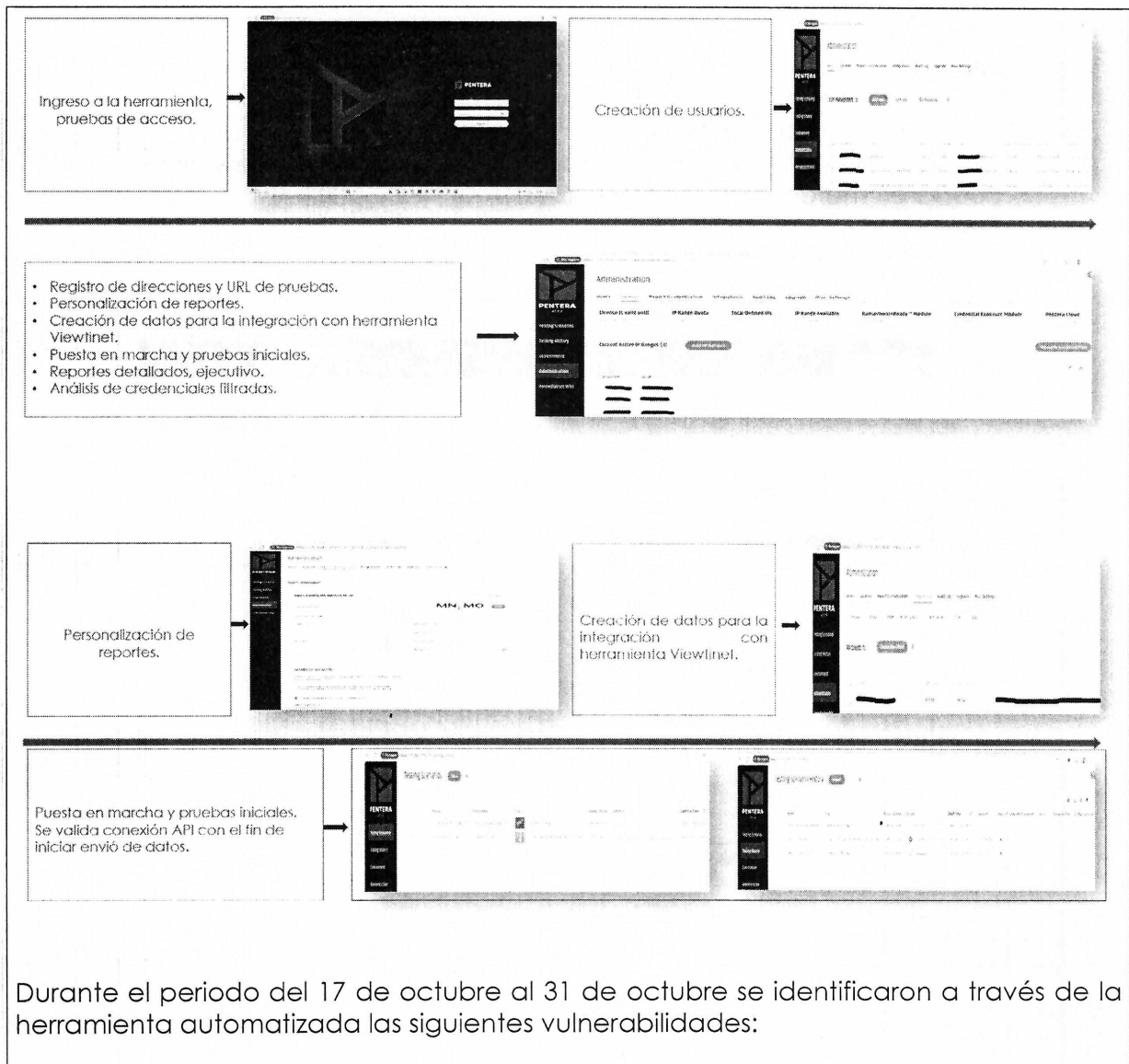
Gráfica: Interfaz de configuración – Solución Seguridad Automatizada.

Implementación

Se realizó el despliegue en una arquitectura cliente – servidor, con la configuración correspondiente, desplegada, se instala el licenciamiento, el proceso se centra en la configuración y acceso a la plataforma vía internet, integración con otros sistemas y validación de la seguridad.

 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



 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



Se generan informes de las pruebas realizadas – Reporte Ejecutivo



Imagen, Informe Postulaciones Jurados.

	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado:
06/06/2017

Es este informe se entrega el análisis realizado sobre el portal de postulación de Jurados, donde se obtiene como resultado la identificación de vulnerabilidades técnicas y las recomendaciones sobre estas.

Este informe es confidencial y de uso exclusivo de la Gerencia Técnica Informática.



Imagen 1. Informe - Sistema tarjetas juvenudes 2025.



Imagen 2. Informe - Sistema registro GSC 2026.

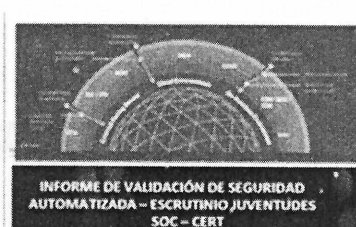


Imagen 3. Informe - Escrutinio juvenudes 2025.

Capacitaciones Jurados Juventudes, Escrutinio De Juventudes Y Sistema Registro Gsc2026

En estos informes se entrega del resultado del análisis realizado al portal tarjetas juvenudes 2025, Escrutinio Juventudes y de Registro GSC 2026, donde se muestran las vulnerabilidades identificadas y las recomendaciones para realizar su respectiva remediación.

Este informe es confidencial y de uso exclusivo de la Gerencia Informática



Imagen 1. Informe Sistema ESCRUTINIO CMLJ



Imagen 2. Informe Sistema PROCESAMIENTO 3 IDC

SISTEMA ESCRUTINIO-CMLJ Y PROCESAMIENTO 3 IDC

El análisis realizado con el hallazgo de vulnerabilidades es una oportunidad para mejorar la resiliencia y madurez en ciberseguridad del sistema. La aplicación de medidas de mitigación, junto con políticas claras de gestión de vulnerabilidades y control de dependencias, permitirá reducir significativamente la superficie de ataque,

	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado:
06/06/2017

proteger la información institucional y fortalecer la confianza de los usuarios en la plataforma. Este informe es confidencial y de uso exclusivo de la Gerencia Informática.



Imagen 1. Informe Sistema Monitoreo y control.



Imagen 2. Informe Sistema DESCARGATUE4.

SISTEMA MONITOREO Y CONTROL Y SISTEMA DESCARGUEUE4

Por medio de estos informe se realiza la entrega del análisis realizado al portal Monitoreo y control y DESCARGAUE4. Donde se muestran las vulnerabilidades identificadas y las recomendaciones para realizar su respectiva remediación. Este informe es confidencial y de uso exclusivo de la Gerencia Informática

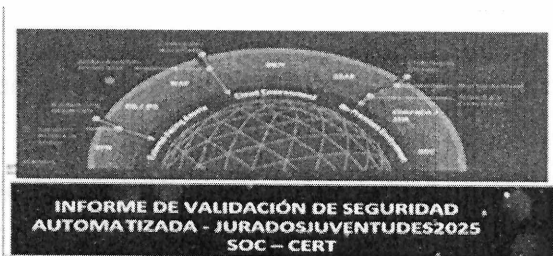


Imagen 1. Informe Sistema JURADOS JUVENTUDES 2025

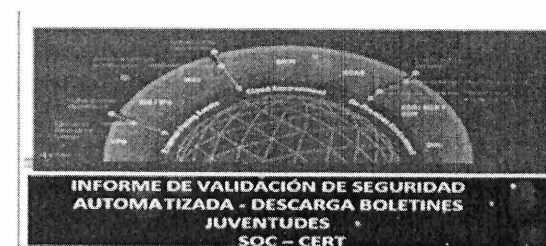


Imagen 2. Informe Sistema DESCARGA BOLETINES JUVENTUDES

SISTEMA JURADOS JUVENTUDES 2025 Y DESCARGA BOLETINES JUVENTUDES

Por medio de estos informe se realiza la entrega del análisis realizado al portal Juradosjuventudes2025 y Descarga Boletines Juventudes. Donde se muestran las vulnerabilidades identificadas y las recomendaciones para realizar su respectiva remediación. Este informe es confidencial y de uso exclusivo de la Gerencia Informática

 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

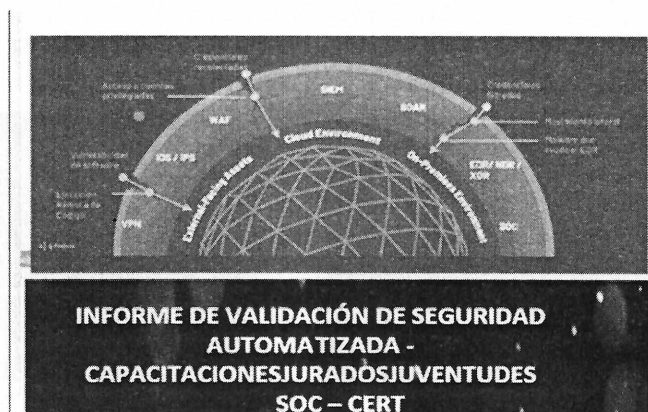


Imagen 1. Informe Sistema capacitaciones jurados juvenudes

Es importante resaltar que la auditoría realizada los sistemas relacionados representa únicamente una fotografía del estado de seguridad 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 segundo pago.

En este Informe de actividades No.2, se describieron los componentes entregados que conforman el pago No. 02.

En esta segunda revisión, se evidencia cumplimiento 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

 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

información para la organización y realización de los procesos electorales a llevarse a cabo en las vigencias 2025 y 2026.

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
SALDO	\$ 33.649.092.315

En constancia de lo anterior, se firma el presente informe, a los diecisiete (17) días del mes de diciembre de 2025.

SUPERVISOR


HOSLANDER ADLAI SÁENZ BARRERA
Gerente de Informática

Proyectó: Juan Alberto Cardona Molina
Revisó: Eduardo Emilio Calderon Narvaez