

 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.	3
PERIODO DE EJECUCIÓN:	01 de diciembre al 31 de diciembre 2025
FECHA PRESENTE INFORME:	31 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. 3.

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. 29265 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

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

Aprobado:
06/06/2017

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

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

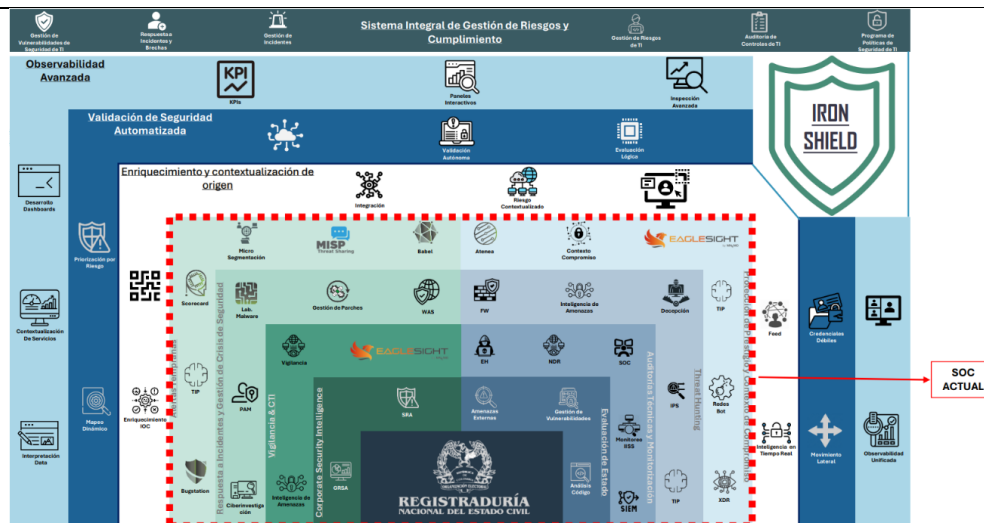
Aprobado:
06/06/2017

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.

 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



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



Gerencia de Informática

Av calle 26 N° 51-50 - teléfono 091 2202880 – Ext. 1526 – CP 11321 – Bogotá

www.registraduria.gov.co

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

Aprobado:
06/06/2017

Enriquecimiento y Contextualización De Origen

- Se realiza la integración con la herramienta de Observabilidad, logrando el envío de datos de consultas.
- Se utiliza la solución en los procesos electorales ejecutados durante este periodo.

Validación de Seguridad Automatizada

- Se efectúa la implementación de la solución, se inicia ajustes y maduración de la solución de la herramienta.
- Se ejecutan pruebas de funcionamiento y puesta a punto.

Observabilidad Avanzada

- Se realiza instalación del appliance en data center de la Registraduría.
- Se realizan reuniones diarias con los responsables de las demás herramientas tecnológicas con el propósito de realizar su integración y despliegue en tableros de control.

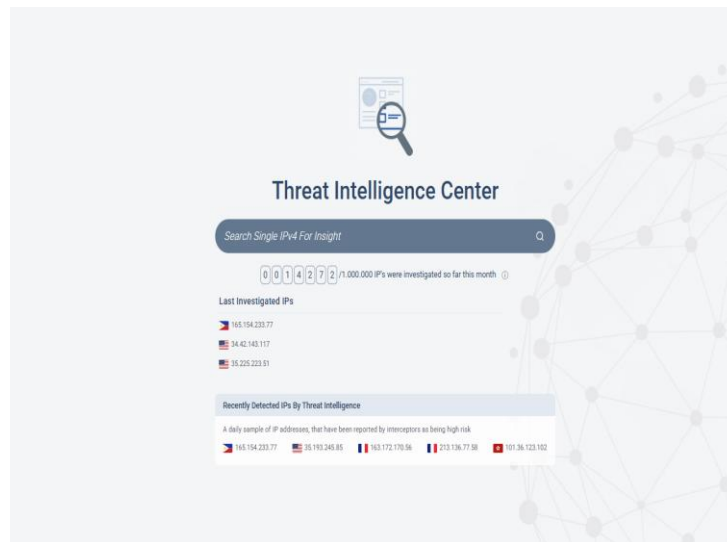
Sistema Integral de Gestión De Riesgos y Cumplimiento

- Se realiza la implementación de la solución y se da inicio al cargue de información en los módulos.
- Se crean y gestionan los usuarios de la solución, de acuerdo a su perfil y responsabilidad.
- Se inicia cargue de información de riesgos y cumplimiento según disponibilidad, así como información de políticas de la entidad.

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

Aprobado:
06/06/2017

1. ENRIQUECIMIENTO Y CONTEXTUALIZACIÓN DE ORIGEN

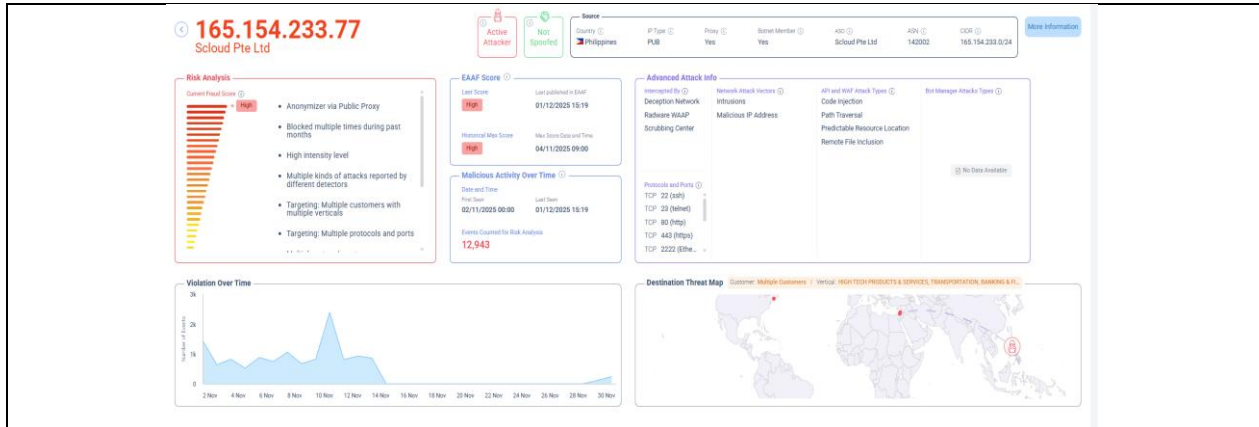


El MÓDULO THREAT INTELLIGENCE CENTER se encarga de detectar, analizar y responder a amenazas cibernéticas en tiempo real utilizando inteligencia avanzada. Este módulo proporciona monitoreo continuo y análisis predictivo mediante inteligencia artificial y análisis de comportamiento para anticipar y mitigar ataques antes de que ocurran, incluyendo amenazas emergentes como vulnerabilidades zero-day y ataques patrocinados por estados. Además, integra la inteligencia de amenazas con otras capas de seguridad para ofrecer una defensa proactiva y automatizada, apoyando la respuesta rápida y detallada ante incidentes de seguridad.

Este módulo también permite correlacionar actividades sospechosas a lo largo del tiempo y en distintas superficies de ataque, ofreciendo una vista unificada del desarrollo de los ataques para detenerlos antes de que resulten en filtraciones de datos o daños mayores. Incluye fuentes de inteligencia global y colaboración con redes internacionales para mantener siempre actualizados los indicadores de amenazas, ayudando a proteger contra ataques volumétricos, bots, DDoS, y ataques dirigidos a la entidad.

 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



El Threat Intelligence Center es una solución integral que utiliza análisis comportamental, aprendizaje automático y datos globales para identificar, alertar y bloquear amenazas de manera anticipada, complementando las defensas existentes con una inteligencia más profunda y automática.



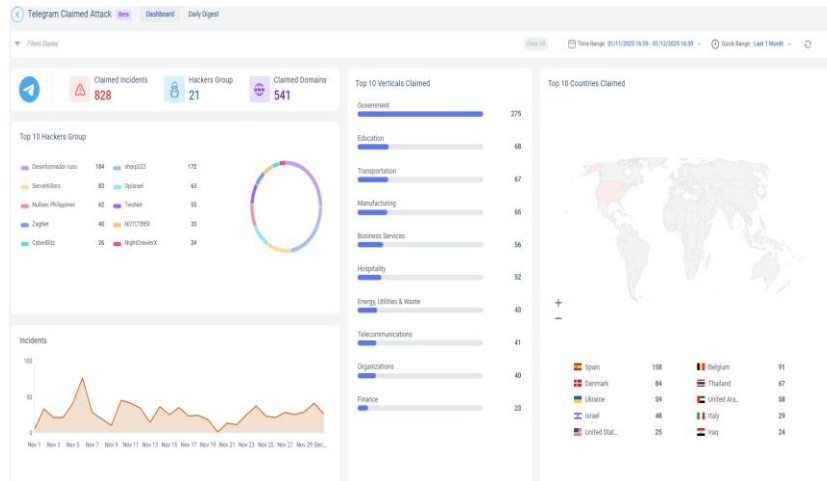
EL MÓDULO LIVE THREAT MAP muestra la información sobre ciberataques a medida que ocurren, basado en la red global de engaño de amenazas y sistemas en la nube de la solución. Este mapa visualiza la actividad de atacantes web, ataques de denegación de servicio (DDoS), intrusiones, escaneos maliciosos y otras amenazas cibernéticas en diferentes partes del mundo. Permite identificar rápidamente cuáles son los países más activos atacando, los servicios que se están atacando (como VNC, SIP, HTTPS) y los métodos de ataque que están siendo usados en ese momento, como ataques UDP flood o TCP flood.

Gerencia de Informática

Av calle 26 N° 51-50 - teléfono 091 2202880 – Ext. 1526 – CP 11321 – Bogotá
www.registraduria.gov.co

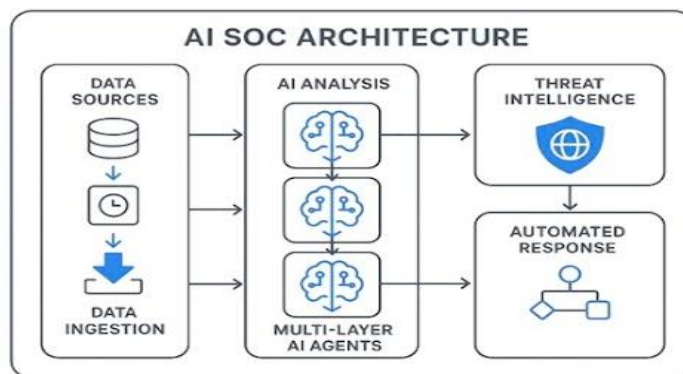
 REGISTRADURÍA NACIONAL DEL ESTADO CIVIL	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado:
06/06/2017



EL MÓDULO TELEGRAM CLAIMED ATTACK proporciona informes en tiempo real sobre ataques cibernéticos que son reivindicados por grupos de hackers a través de la plataforma Telegram. Este módulo recopila y analiza automáticamente las comunicaciones y reclamos de ataques compartidos en canales de Telegram para ofrecer visibilidad inmediata sobre amenazas específicas dirigidas a regiones, sectores o víctimas determinadas.

Este servicio permite a los equipos de seguridad anticiparse a ataques potenciales al conocer detalles sobre el tipo, alcance y evidencia del ataque que grupos hacktivistas publican, ayudando a tomar medidas proactivas para mitigar riesgos. El panel de información se actualiza cada 15 minutos, permitiendo un monitoreo continuo que mejora la preparación y respuesta de los centros de operaciones de seguridad (SOC).



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

Aprobado:
06/06/2017

Se habilitó el módulo de Threat Intelligence Feed dentro del ecosistema, activando las capacidades de detección, análisis de amenazas globales y clasificación de indicadores de compromiso.

Esto incluyó la configuración inicial del servicio, la validación de licenciamiento y la sincronización con la infraestructura principal.

Durante este periodo se ha hecho entrega de

- 5 informes mensuales de la operación del Servicio:

SOC Electoral 2025 > ENTREGABLES > 5. INFORMES > 1. ENRIQUECIMIENTO DE ORIGEN > NOVIEMBRE

Nombre	Modificado	Modificado por
 20251109 - Enriquecimiento y contextualización de origen - Elecciones Atípicas Villeta Cundinamarca.pdf	Hace unos segundos	Yenny Fernanda Hernandez Perez
 20251123 - Enriquecimiento y contextualización de origen - Gobernador Magdalena.pdf	El martes a las 16:35	Yenny Fernanda Hernandez Perez
 20251130 - Enriquecimiento y contextualización de origen - Proceso Derogatorio Paz De Aripuro.pdf	hace 8 horas	Yenny Fernanda Hernandez Perez
 Análisis de origen 091125.pdf	10 de noviembre	James Gustavo Arana Reyes
 informe atipicas.xlsx	El lunes a las 16:09	Yenny Fernanda Hernandez Perez
 URLs proceso electoral Villeta - Cundinamarca.xlsx	18 de noviembre	Juan Alberto Cardona Molina

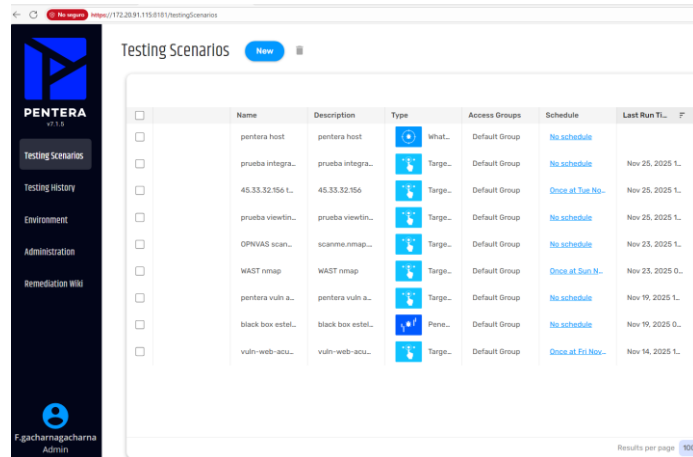
2. VALIDACIÓN DE SEGURIDAD AUTOMATIZADA

Descripción de la Capacidad:

- 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.

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

Aprobado:
06/06/2017



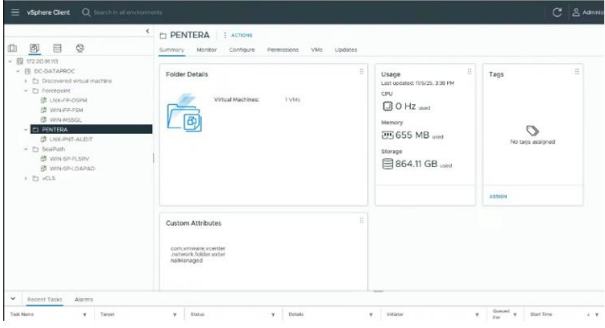
	Name	Description	Type	Access Groups	Schedule	Last Run TL	F
☐	pentra host	pentra host	what...	Default Group	No schedule	Nov 25, 2025 1.	
☐	prueba integra...	prueba integra...	Target...	Default Group	No schedule	Nov 25, 2025 1.	
☐	45.33.32.156 L...	45.33.32.156	Target...	Default Group	Once at Tue No...	Nov 25, 2025 1.	
☐	prueba viewfin...	prueba viewfin...	Target...	Default Group	No schedule	Nov 25, 2025 1.	
☐	OPNVAS scan...	scanme.nmap...	Target...	Default Group	No schedule	Nov 23, 2025 1.	
☐	WAST nmap	WAST nmap	Target...	Default Group	Once at Sun, N...	Nov 23, 2025 0...	
☐	pentra vuln a...	pentra vuln a...	Target...	Default Group	No schedule	Nov 19, 2025 1.	
☐	black box extel...	black box extel...	Prime...	Default Group	No schedule	Nov 19, 2025 0...	
☐	vuln-web-acu...	vuln-web-acu...	Target...	Default Group	Once at Fri Nov...	Nov 14, 2025 1.	

Detalle de la implementación:

- La herramienta en la versión 7.1.5, se instaló en plataforma ESXi, en máquina virtual ubicado en datacenter de RNEC, dirección IP correspondiente, con sistema operativo Ubuntu Ver. 22.04.
- El reloj interno se ha sincronizado con el Directorio Activo de RNEC, 172.20.60.170 y está en proceso de activación de 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.
- Se han hecho pruebas exitosas de integraciones mediante API y mediante Syslog y se ha construido un primer tablero de resumen de cantidad de pruebas, y cantidad de tareas por tipo y por estado.
- Esta en desarrollo un gráfico de disponibilidad del servicio.
- Se ha validado el proceso de copia de respaldo con la herramienta Veeam backup a mediano plazo, actualmente se respalda la máquina virtual con una copia tipo snapshot desde el 27-11-2025.
- Se han realizado diversas pruebas exitosas de pentesting y reportes.

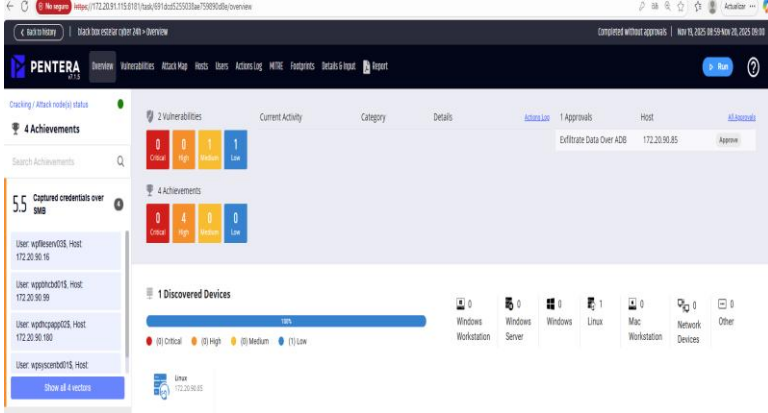
 REGISTRADURÍA NACIONAL DEL ESTADO CIVIL	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado:
06/06/2017




Se verificó técnicamente el proceso de aseguramiento del fabricante respecto a:

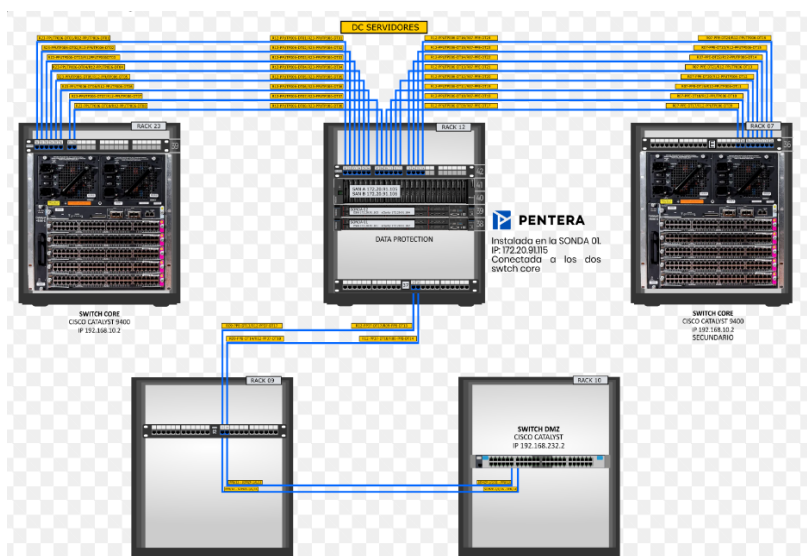
- Usuario root
- Comandos de alto privilegio restringido
- Soporte de protocolos de red innecesarios eliminado
- Compatibilidad con sistemas de archivos innecesarios desactivada
- Desinstalación de paquetes comunes
- Volcados de Kernel desactivados
- Algoritmo por defecto de contraseñas actualizado
- Política estricta de contraseñas
- Creación de llaves pública y privada para conexión SSH



 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 solución se ubica en la VLAN 172.20.91.XXX, 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.



La licencia CORE, cubre 3.000 direcciones IP internas, incluye módulo de simulación de ramsonware, módulo de prueba de contraseñas de directorio activo y contraseñas filtradas. Incluye pruebas OWASP TOP 10 para dominios TLD

Durante este periodo se ha hecho entrega de

- 2 informes mensuales de la operación del Servicio:

SOC Electoral 2025 > ENTREGABLES > 5. INFORMES > 2. VALIDACIÓN SEGURIDAD AUTOMATIZADA > DICIEMBRE

Nombre	Modificado	Modificado por
 Validación de Seguridad Automatizada – Informe Credenciales filtradas.pdf	hace 6 horas	Yenny Fernanda Hernandez Perez
 Validación de Seguridad Automatizada – Implementación de la Solución.pdf	hace 6 horas	Yenny Fernanda Hernandez Perez

Gerencia de Informática

Av calle 26 N° 51-50 - teléfono 091 2202880 – Ext. 1526 – CP 11321 – Bogotá

www.registraduria.gov.co

 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

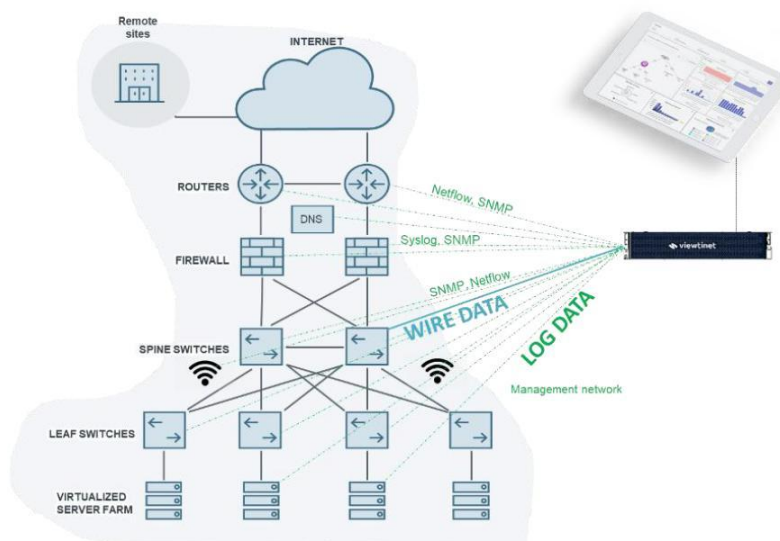
3. OBSERVABILIDAD AVANZADA

La solución de Observabilidad Avanzada, propone una solución capaz de aportar no sólo analítica avanzada del tráfico IP, sino, además, como mejora sustancial, de analizar cualquier log y métrica de cualquiera de los fabricantes existentes en la red. El mismo appliance es capaz de recibir el tráfico, recibir los logs, analizarlos, almacenarlos, procesarlos y aportar analítica avanzada, monitorización y alarmas.

Una ventaja de la solución es que es capaz de incorporar logs y métricas de cualquier fabricante, en cualquier formato. Esto es muy útil para numerosos casos de uso:

Monitorización de red y extracción de KPIs de dispositivos mediante SNMP, ICMP, etc.

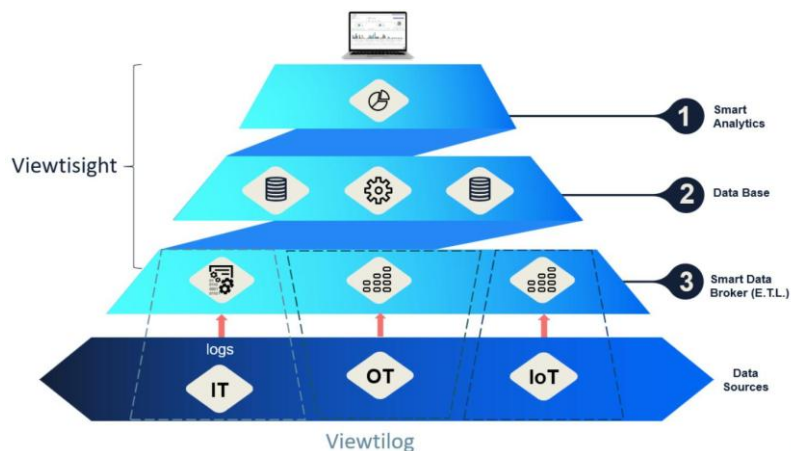
- Monitorización y analítica de tráfico Netflow.
- Integración con APIs para analítica.
- Monitorización de servidores por WMI.
- Analítica avanzada de eventos de seguridad por Syslog.



Esta capacidad va incluida en el producto propuesto. Hasta 700GB/día de ingesta de logs al día y la integración de cualquier fuente estándar del Ecosistema IT va incluido en la licencia.

 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



Analítica avanzada – Cuadros de mando – Alarmas – Reportes automatizados

La solución se destaca también por su motor gráfico. Todos los productos cuentan con cuadros de mando predefinidos, visuales e interactivos. Ahora bien, configurar nuevos cuadros de mando o editar los ya existentes se realiza de forma fácil e intuitiva.

Cuenta con un asistente para poder realizar cualquier reporte a un click, aportando información de las métricas y dimensiones disponibles. No es preciso introducir ninguna query y los usuarios se benefician de una curva de aprendizaje muy rápida.

Todos los reportes son interactivos. Se permite hacer drill-down en cada uno de los campos de modo que se pueda navegar en la información y hacer troubleshooting de manera óptima.

Su panel de alarmas y notificaciones permite además numerosas reglas para incluso realizar correlaciones de diferentes eventos o umbrales, así como realizar acciones como envío de e-mails, notificaciones de eventos, envío de mensajes de WhatsApp, envío de mensajes de Slack, scripts, etc. Las alarmas se muestran también en una interfaz intuitiva donde se puede visualizar la información y realizar diferentes acciones.

Permite incluso configurar el envío de reportes automatizados en pdf, de modo que se pueda seleccionar qué gráficos incluir, a quién se envían y con qué periodicidad.

El panel de configuración de la solución es muy granular respecto a los permisos de

 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

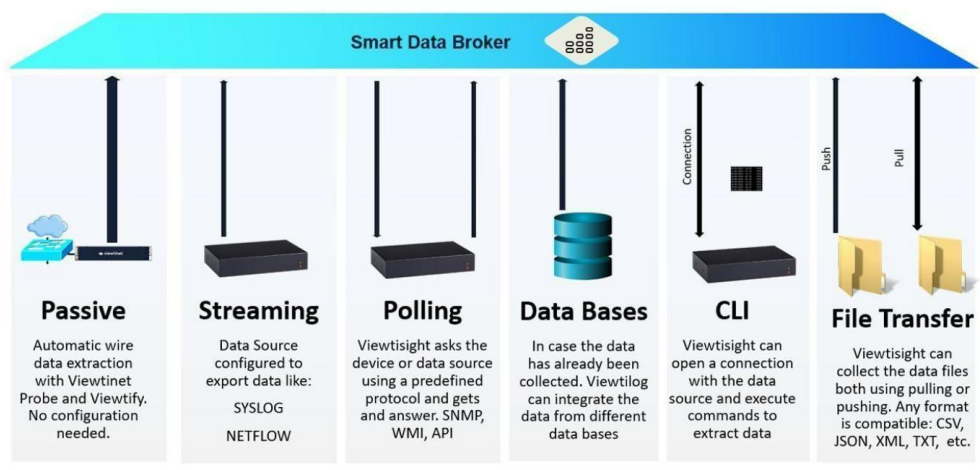
los usuarios que tienen acceso de la herramienta. Se permiten permisos de modo que dependiendo del usuario teniendo posibilidad o no de editar cuadros de mando, además, se permite que según qué usuario tenga accesos a unos determinados datos, o subredes y a otros no.

Despliegue RNEC

La solución implementada en la entidad se basa en la plataforma de Observabilidad avanzada, la cual integra tecnologías de Observabilidad orientadas a la recopilación, normalización y análisis de datos provenientes de diversas fuentes operativas. La herramienta permite la ingesta de información mediante protocolos estándar como Syslog, APIs y otros mecanismos de consulta, facilitando así la consolidación de eventos, métricas y registros generados por los sistemas del entorno.

La plataforma incorpora módulos especializados para la gestión de logs y la visualización de indicadores clave, permitiendo al equipo técnico acceder a cuadros de mando dinámicos, reportes ejecutivos y alertas configurables. Gracias a su motor gráfico y de procesamiento, la tecnología soporta altas cargas de información y ofrece capacidad de análisis en tiempo real.

El sistema se ejecuta sobre un appliance dedicado que proporciona estabilidad, rendimiento y los recursos necesarios para garantizar una operación continua del servicio y el adecuado procesamiento de los datos integrados.



 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

Detalle de la implementación

En la fase de implementación se tiene como ruta inicial la integración de cuatro (4) fuentes de datos, entre ellas QRadar (SIEM). Esto se hará en base a los diferentes mecanismos y protocolo de recepción de tráfico y datos como lo son Syslog y vía API. Para esto se hará uso de los módulos mas precisos con los que cuenta la solución para dicho desarrollo, como se muestran a continuación:

- Modulo para monitoreo de dispositivos vía protocolo syslog.
- Modulo para gestión la visualización de cuadros de mando, alertas y reportes.

Arquitectura

Los datos para construir una red inteligente ya existen en la infraestructura actual (servidores, enrutadores, switches, etc.), pero a menudo están subutilizados. Estos datos, que provienen de registros en formatos diversos, necesitan ser transformados y analizados para ofrecer información útil en tiempo real. Esto permite actuar rápidamente y mejorar la experiencia del usuario, especialmente con la creciente cantidad de dispositivos IoT y comunicación M2M. La combinación de datos de registro y tráfico real es crucial para un diagnóstico efectivo de la red.

Licencia

- Módulos
- Monitoreo para 7000 dispositivos
- Ingesta de data de 700GB por día
- Soporte hasta el 12 de octubre de 2026

Configuración (Hardware y Servicios)

La solución fue implementada sobre un appliance físico destinado exclusivamente para el monitoreo y la gestión del entorno de red definido en el alcance del proyecto.

Detalles del Hardware

El dispositivo corresponde a un servidor modelo VN-2000-HW-Base-40G-AC, identificado con el número de serie VN-0050025-01-025867, cuyas especificaciones

 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

técnicas son las siguientes:

Especificaciones	
Factor de forma	Appliance 1 RU
Memoria RAM	256 GB
Discos del sistema	2 × 960 GB
Discos de base de datos	4 × 3.8 TB
Puerto de administración (IPMI)	1 × RJ45
Interfaces de red	4 × SFP+ (1/10G)
Fuente de poder	AC

Estas características garantizan el rendimiento necesario para la gestión y procesamiento de los datos recolectados por la plataforma, asegurando una adecuada capacidad de almacenamiento, disponibilidad y velocidad de consulta para los distintos módulos operativos de la herramienta.

Entorno Operativo

El appliance ejecuta el sistema operativo Ubuntu Server 24.04.2 LTS, entorno sobre el cual se despliegan los componentes principales, incluyendo los servicios de base de datos, monitoreo, motor de correlación y la interfaz web de administración. Este entorno provee estabilidad, soporte a largo plazo y compatibilidad con los servicios requeridos por la solución, permitiendo una operación continua y confiable.

Configuración Operativa de la Herramienta

A nivel de software, la plataforma fue implementada en su última versión estable, correspondiente a la v6.3.5, bajo el release Build v6.3.5.4612, publicado el 10 de noviembre de 2025.

Esta versión incorpora las últimas mejoras en rendimiento, estabilidad y seguridad, así como nuevas funcionalidades en los módulos de análisis, visualización y gestión de métricas.

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

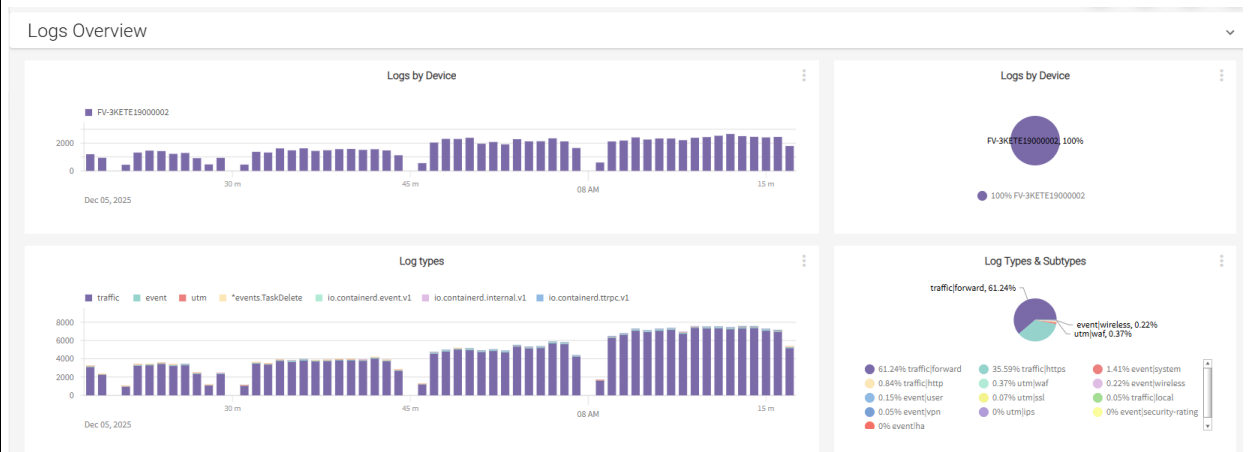
Aprobado:
06/06/2017

Integraciones

Para el presente periodo, se desarrollaron las integraciones de las diferentes herramientas de la solución IronShield, con la herramienta de Observabilidad avanzada, esta integraciones permiten a la Entidad, facilitar analítica avanzada con la presentación de tableros de control (dashboards) para obtener visibilidad ejecutiva.

integración con la herramienta Enriquecimiento y Contextualización de Origen

La estrategia de integración permite el consumo de datos desde la herramienta de Enriquecimiento y Contextualización de Origen API, fundamentada en la consulta del endpoint Threat Intelligence / Bulk Resolve de direcciones IP. Esto permite al sistema de Observabilidad obtener y procesar los eventos y registros (logs) específicos relacionados con cada dirección IP resuelta.



Lo fundamental de esta interacción es que la respuesta del endpoint, proporciona inteligencia de amenazas directamente asociada a cada IP, la cual se traduce en indicadores de compromiso (IoCs). Esta información es crítica porque incluye una serie de atributos que definen el perfil de riesgo de la IP, tales como:

- Clasificación de riesgo: si la IP es maliciosa o presenta mala reputación.
- Historial de actividad: si ha participado en ataques o ha generado eventos previos.
- Afiliaciones: si pertenece a botnets o está asociada a fraude.
- Estatus de bloqueo: si está en listas negras.
- Categorías de amenaza detalladas.

 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 consolidación de todos estos atributos en la plataforma confirma la ingesta de valiosos indicadores de compromiso (IoCs) para el análisis de seguridad.

integración con la herramienta de validación de Seguridad Automatizada.

La estrategia de consumo, en este caso, se ha llevado a cabo mediante la integración con la API de la herramienta tecnológica de validación de Seguridad Avanzada, se ejecuta mediante la consulta específica del endpoint Testing_History. La finalidad de esta conexión es la ingesta de los informes de resultados derivados de las evaluaciones de seguridad de la plataforma.

La solución destinada para validación de seguridad automatizada, simula escenarios de ataque y amenaza de manera proactiva. Al utilizar un identificador único de la tarea (task ID) recuperado del endpoint Testing_History, la solución de Observabilidad puede correlacionar los hallazgos de forma precisa para construir un mapa relacional de las vulnerabilidades identificadas en el entorno.

Durante este periodo se ha hecho entrega de

- 3 informes mensuales de la operación del Servicio:

SOC Electoral 2025 > ENTREGABLES > 5. INFORMES > 3. OBSERVABILIDAD AVANZADA

Nombre ▾	Modificado ▾	Modificado por ▾
 INFORME DE IMPLEMENTACIÓN - OBSERVABILIDAD AVANZADA.pdf	hace 3 minutos	Yenny Fernanda Hernandez Perez
 INFORME EJECUTIVO - OBSERVABILIDAD AVANZADA IMPLEMENTACIÓN.pdf	hace 3 minutos	Yenny Fernanda Hernandez Perez
 INFORME TÉCNICO - OBSERVABILIDAD AVANZAD IMPLEMENTACION.pdf	hace 3 minutos	Yenny Fernanda Hernandez Perez

 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

4. SISTEMA INTEGRAL DE GESTIÓN DE RIESGOS Y CUMPLIMIENTO

Plataforma en Nube. La cual, tiene una Arquitectura multicapa (3-tier), arquitectura orientada a servicios dentro de la plataforma. Donde, se cuenta con:

- Capa de Presentación: interfaz web.
- Capa de Aplicación: lógica del negocio.
- Capa de Base de Datos: almacenamiento estructurado.

Está estructurado en módulos: riesgos, controles, vulnerabilidades, incidentes, Auditoría; en general Gobernanza, Cumplimiento, Riesgos. Seguridad de la Información.

Servicios:

- Cumplimiento.
- Gobernanza.
- Gestión de Riesgos.
- Gestión de Incidentes de Ciberseguridad.
- Gestión de Vulnerabilidades.
- Continuidad de servicio.

En nube para la prestación del proyecto se dispone de 10 GB de almacenamiento por cada una de las instancias.

La solución es configurable de acuerdo con las necesidades de la RNEC que permite a nivel de plataforma construir, configurar, operar y escalar cualquier proceso GRC.

- Modelado de Aplicaciones: Diseñar aplicaciones sin código, Tablas, formularios, workflows y campos personalizados.
- Workflows Avanzados: Modelación de procesos, aprobaciones y rutas condicionales, automatizaciones.

Implementación:

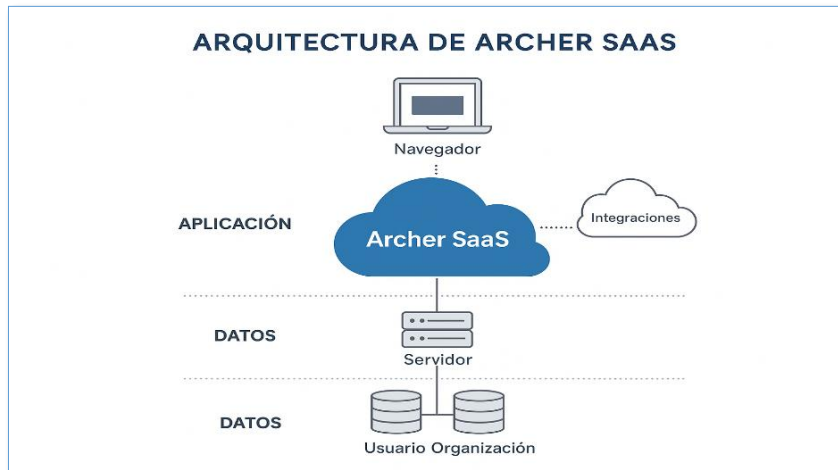
Solución SaaS:

Habilitación de las Instancias: **durante este periodo se habilitaron las siguientes instancias** Producción, pruebas y Desarrollo, permitiendo el inicio de los cargues de información de la entidad.

 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

Solución SaaS.



Instancias:

Instancias de SaaS

- 1 Productiva (PRD)
Número de Instancia (PIN) [REDACTED]
<https://registraduria.archerirm.us>
- 1 No Productivas (TEST)
Número de Instancia (PIN) [REDACTED]
<https://registraduria-test.archerirm.us>
- 1 No Productivas (DEV)
Número de Instancia (PIN) [REDACTED]
<https://registraduria-dev.archerirm.us>
- Cada Instancia tiene una cuenta FTP (10 GB almacenamiento)

4 | ©2021 Archer Technologies LLC. All rights reserved. 

La herramienta del Sistema Integral de Gestión de Riesgos y Cumplimiento, para mejores prácticas por entorno, presenta tres instancias:

- **Desarrollo (Dev):** Usa configuraciones single-host (donde un solo servidor físico aloja tanto el tier web (aplicación web) como el tier de base de datos)) para prototipos rápidos, entrenamiento o pruebas iniciales de workflows y campos personalizados.

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

Aprobado:
06/06/2017

- Pruebas (Test): Replica estructuras de producción con datos anonimizados; ideal para validar integraciones, reportes y accesos.
- Producción (Prod): Implementa multi-servidor con alta disponibilidad, base de datos separada y firewalls dobles; evita sobrecargas escalando roles independientemente.

Módulo de Riesgo:



La imagen muestra la interfaz de usuario del módulo de riesgos en la plataforma ARCHER. El encabezado indica 'Resultados de búsqueda: Carga - Riesgos'. La tabla de resultados contiene la siguiente información:

Riesgo	Estado	Clasificación De Riesgo	¿Qué? Impacto	¿Cómo? Causa Inmediata
RSK-2025-001	Activo	Operativo	Posibilidad de afectación económica y/o reputacional	Por retrasos y/o incumplimientos en la entrega de informes ejecutivos, de gestión o entregables al cliente
RSK-2025-002	Activo	Operativo	Posibilidad de afectación económica y/o legal	por errores en la ejecución operativa de los servicios SOC-CERT referentes a la (implementación del servicio, metodologías, procesos, procedimientos, fallas en la coordinación de equipos)

La gráfica ilustra la inclusión de los riesgos identificados en los servicios implementados en el SOC-CERT en la plataforma; en el diseño se incluyó las características necesarias en la identificación de los riesgos operativos y de seguridad de la información.

En este módulo de riesgos permitira identificar, evaluar, responder y monitorear riesgos operativos de forma centralizada, alineándolos con objetivos de negocio.

Dentro de las funciones principales, se encuentran:

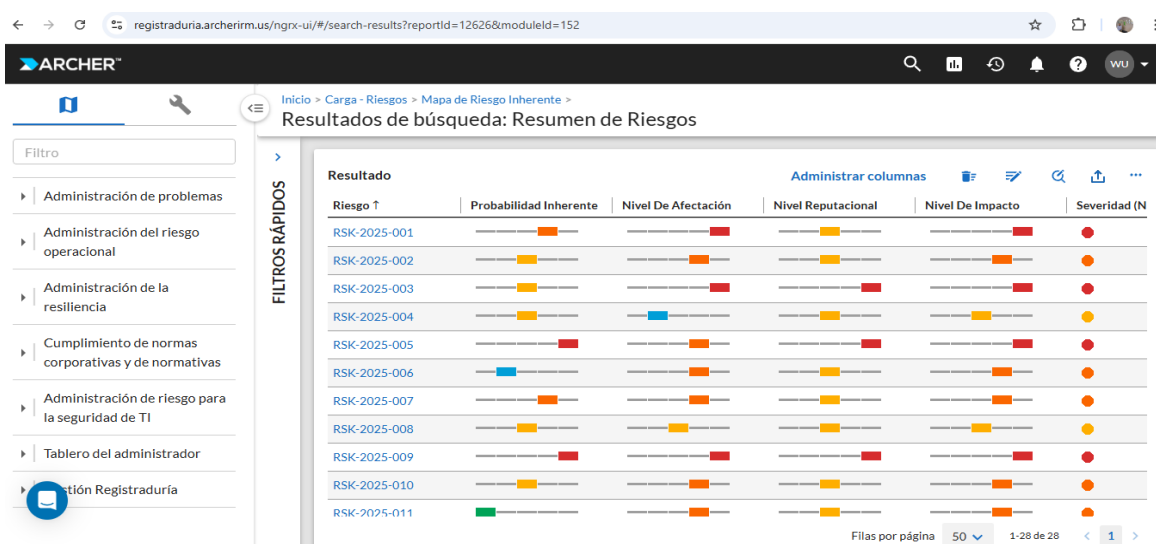
- Registro de Riesgos: Crea y mantiene un risk register con jerarquías, métricas de riesgo y eventos de pérdida para análisis cualitativo y cuantitativo.

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

Aprobado:
06/06/2017

- Evaluaciones y Campañas: Gestiona campañas de autoevaluación, scoring y workflows drag-and-drop para las "tres líneas de defensa" (negocio, gestores de riesgo, auditoría).
- Monitoreo y Reportes: Ofrece tableros personalizados, informes out-of-the-box, análisis y alertas para visibilidad en tiempo real de exposición al riesgo.

Dentro de los beneficios de la solución, se encuentra la integración con incidentes y cumplimiento normativo, llevando con ello a un mejor control para la toma de decisiones estratégicas en riesgos IT.



La herramienta del Sistema Integral de Gestión de Riesgos y Cumplimiento permite tener una visualización de los riesgos identificados en los servicios del SOC-CERT, observándose el nivel de probabilidad inherente, nivel de afectación, nivel reputacional, nivel de impacto y severidad del riesgo.

Módulo de Políticas:

La herramienta tecnológica del Sistema Integral de Gestión de Riesgos y Cumplimiento Incluye el módulo de políticas que permite crear, distribuir, gestionar y monitorear políticas de la entidad de forma centralizada, asegurando alineación con normativas y controles internos.

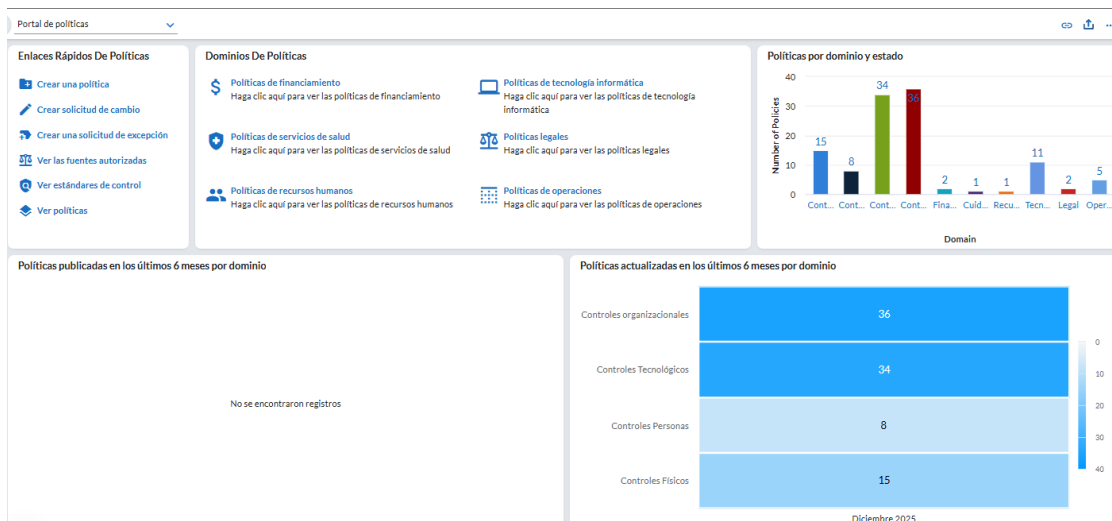
 REGISTRADURÍA NACIONAL DEL ESTADO CIVIL	PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
	FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORÍA	VERSIÓN	0

Aprobado:
06/06/2017

Dentro de sus funciones, se encuentra:

- **Gestión de Políticas:** Almacena políticas en un repositorio unificado, con versiones, aprobaciones workflows y asignación a dueños/áreas para cumplimiento continuo.
- **Evaluaciones y Controles:** Vincula políticas a controles, riesgos y evaluaciones, facilitando auditorías, pruebas de cumplimiento y reportes automatizados.
- **Distribución y Lectura:** Envía políticas por email o portal, rastrea confirmaciones de lectura y capacitación, integrando con las tres líneas de defensa.

Adicionalmente, automatiza el ciclo de vida de políticas para mitigar riesgos de incumplimiento, mejora visibilidad ejecutiva vía dashboards y soporta integraciones con riesgos IT.



Durante este periodo, se ha dado inicio al cargue de las políticas o lineamientos establecidos por la Registraduría Nacional del Estado Civil – RNEC en el manual PGMN01 MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, se encuentran cargadas en la herramienta de gestión. Estos lineamientos se encuentran clasificados en cuatro (4) dominios de control según la norma ISO 27001/2022:

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

Aprobado:
06/06/2017

- Controles Organizacionales
- Controles Físicos
- Controles de Personas
- Controles Tecnológicos

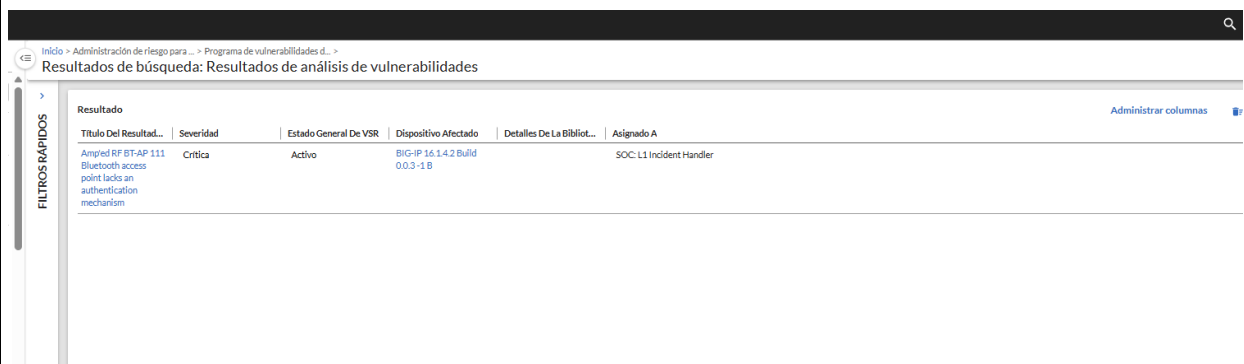
Módulo de vulnerabilidades:

Este módulo de vulnerabilidades de seguridad de TI, permite a analistas identificar, analizar y remediar vulnerabilidades mediante alertas automatizadas y exploración de resultados de escaneos.

Como Funciones a destacar se encuentra:

- Gestión de Vulnerabilidades: Implementa alertas, explora hallazgos de análisis de vulnerabilidades y prioriza problemas para aumentar el índice de cierre de brechas críticas.
- Análisis y Reportes: Analiza vulnerabilidades emergentes, integra con riesgos IT y genera tableros para monitoreo en tiempo real.
- Integración GRC: Vincula vulnerabilidades a riesgos, políticas y incidentes, soportando workflows para las tres líneas de defensa y cumplimiento normativo.
- Beneficios en Seguridad IT.

Estas características mejoran la respuesta a amenazas cibernéticas, reduce exposición al mitigar brechas rápidamente y proporciona visibilidad centralizada.



vicio > Administración de riesgo para ... > Programa de vulnerabilidades d... >					
Resultados de búsqueda: Resultados de análisis de vulnerabilidades					
Resultado	Severidad	Estado General De VSR	Dispositivo Afectado	Asignado A	
Amplified RF BT-AP 111 Bluetooth access point lacks an authentication mechanism	Crítica	Activo	BIG-IP 16.14.2 Build 0.0.3-1 B	SOC: L1 Incident Handler	

La grafica muestra, como se presenta la información de vulnerabilidades en la herramienta de gestión.

 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

Es importante resaltar que la auditoría realizada a 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 tercer pago.

En este Informe de actividades No.3, se describieron los componentes entregados que conforman el pago No. 03.

En esta tercera 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 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:

 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

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
SALDO	\$ 28.871.893.845

En constancia de lo anterior, se firma el presente informe, a los treinta y un (31) días del mes de diciembre de 2025.

SUPERVISOR



HOSLANDER ADLAI SÁENZ BARRERA
Gerente de Informática

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