

 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

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.	1
PERIODO DE EJECUCIÓN:	10 de octubre al 31 de octubre 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. 1.

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) Observabilidad Avanzada, c) Validación de seguridad automatizada y d) Sistema Integral de Gestión de Riesgos y Cumplimiento.

Descripción (Bienes y Servicios)
a) Enriquecimiento y contextualización de origen
b) Observabilidad Avanzada
c) Validación de seguridad automatizada
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.

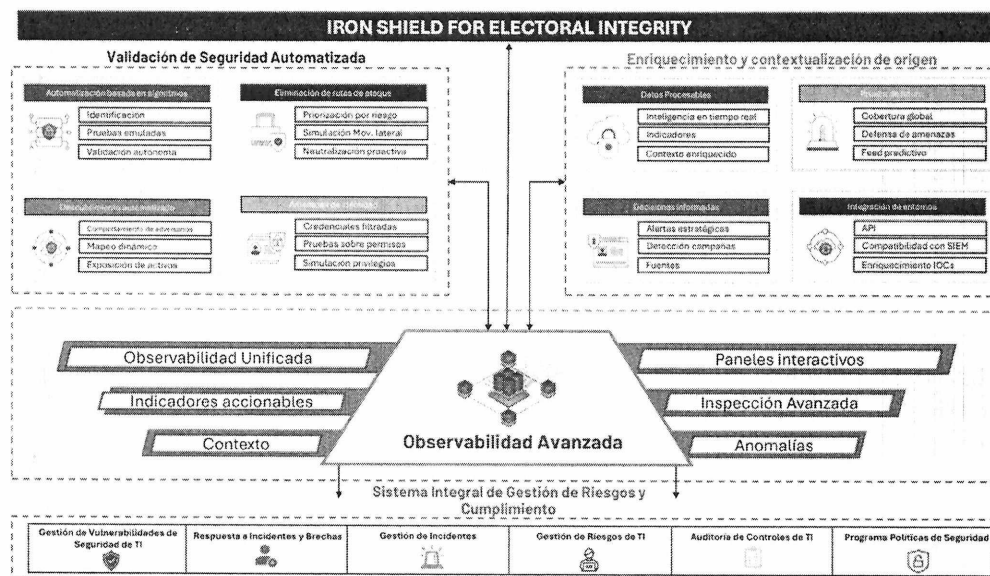
El servicio Iron Shield for Electoral Integrity tiene como propósito establecer un servicio integral de ciberseguridad (por la vigencia del contrato) orientado a fortalecer, ampliar y sofisticar las capacidades actuales del Centro de Operaciones de Seguridad (SOC), con un enfoque específico en la protección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

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

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

Aprobado:
06/06/2017

integral, orientada a la anticipación, mitigación y respuesta efectiva frente a amenazas cibernéticas.



Los pilares que estructuran el servicio son los siguientes:

ENRIQUECIMIENTO Y CONTEXTUALIZACIÓN DE ORIGEN

Este pilar permite transformar datos crudos de amenazas en inteligencia procesable mediante la integración de fuentes OSINT y de datos externos. Su propósito es identificar, en tiempo real, comportamientos maliciosos, direcciones IP involucradas en ataques (como DDoS o botnets), y campañas dirigidas a regiones específicas. Así mismo, contribuye a la detección de afirmaciones y amenazas provenientes de actores maliciosos en entornos de comunicación clandestina.

OBSERVABILIDAD AVANZADA

Este componente proporciona visibilidad en tiempo real a través de la colección e interpretación de datos de cualquier componente tecnológico provenientes de diversas fuentes como Netflow, Syslog, SNMP, WMI, API, CDR, XML y CSV, incluyendo flujos cifrados, permitiendo la detección de amenazas avanzadas como movimientos laterales. Integra la correlación entre eventos del SIEM y datos observables, validación de grandes volúmenes de indicadores de compromiso (IoCs) y facilitando la recolección de evidencia forense. Esta capacidad permite acelerar investigaciones y priorizar incidentes de manera estratégica.

 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

VALIDACIÓN DE SEGURIDAD AUTOMATIZADA

A través de pruebas de penetración continuas, simulación de ataques reales y automatización de escenarios de intrusión, este componente permite detectar y corregir proactivamente vulnerabilidades críticas en la infraestructura tecnológica. La emulación del comportamiento adversario permite identificar rutas potenciales de ataque antes de que sean explotadas, fortaleciendo de forma anticipada la postura de seguridad.

SISTEMA INTEGRAL DE GESTIÓN DE RIESGOS Y CUMPLIMIENTO

Este componente proporciona una visión centralizada y en tiempo real de los riesgos de ciberseguridad, permitiendo a las entidades responsables de los procesos electorales tomar decisiones informadas. Facilita la automatización de procesos de cumplimiento, centraliza políticas y procedimientos, garantiza trazabilidad y auditabilidad, y permite el monitoreo continuo de activos críticos, apoyado en capacidades analíticas avanzadas. La integración de estos pilares bajo una única arquitectura operativa permite garantizar una cobertura amplia y profunda frente al panorama de amenazas cibernéticas, reforzando la confianza en los procesos electorales y alineando las capacidades del SOC con los más altos estándares de ciberseguridad aplicados a infraestructuras críticas.

 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

SOC Electoral 2025 > ENTREGABLES > 1. ACTAS

Nombre

Modificado

Modificado por

Acta de Inicio Servicio Iron Shield.pdf

28 de octubre

James Gustavo Arana Reyes

FIRMA DE REVISIÓN Y ANÁLISIS DE HOJAS DE VIDA DEL SERVICIO

Se realizó la Revisión de las Hojas de vida de los profesionales asignados al servicio 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. Se deja evidencia en el acta No 001

CANT	CARGO	PERFIL
1	LIDER DE AUDITORIA AUTOMATIZADA	Profesional — universitario en ingeniería de sistemas, telecomunicaciones, electrónica o afines. Certificación CHFI Computer Hacking Forensic Investigator, Cinco años de experiencia en seguridad de la información.
1	AUDITORÍA AUTOMATIZADA	Profesional universitario en ingeniería de sistemas, telecomunicaciones, electrónica o afines. Especialización en ciberseguridad, Certificación en Ethikal Hacker CEH. Certified Web Applicatio Expert. Cinco años de experiencia en auditoría de la información.
1	LÍDER GRS	Profesional universitario en ingeniería de sistemas, telecomunicaciones, electrónica o afines. Especialización o magister en ciberseguridad o auditoría de sistemas. Certificación en Lead Risk Manager ISO 31000:2018, Auditor Interno ISO 27001:2022. Certified ISO 27005 Risk Manager. Tres años de experiencia en actividades relacionadas con seguridad de la información.
1	CYBER THREAT INTELLIGENCE	Profesional universitario en ingeniería de sistemas, telecomunicaciones, electrónica o afines. Certificación en CTIA - Certified Threat Intelligence Analyst Internal Auditor. ISO 27001-2022. Tres años de experiencia en actividades relacionadas con inteligencia de amenazas.
1	INTELIGENCIA ARTIFICIAL	Profesional universitario en ingeniería de sistemas, telecomunicaciones, electrónica o afines. Especialista en seguridad de la información Certificación en Artificial ntelligence Professional Certificate -CAIPC. — Cybersecurity - Awareness — Professional Certification CAPC, Lead Cybersecurity Professional Certification. LCSPC. Dos años de experiencia en actividades de ciberseguridad.

 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

SOC Electoral 2025 > ENTREGABLES > 1. ACTAS

Nombre	Modificado	Modificado por
Acta de Inicio Servicio Iron Shield.pdf	28 de octubre	James Gustavo Arana Reyes
ACTA DE REVISIÓN DE HOJAS DE VIDA DEL SERVICIO IRONSHIELD - RNEC.pdf	29 de octubre	James Gustavo Arana Reyes

ADQUISICIÓN DE LICENCIAMIENTO

Dentro del proceso de para la puesta en funcionamiento, se realizó la adquisición de las herramientas tecnológicas para atender los pilares que soportaran los servicios.

Item	Product Name	Quantity	Start Date	End Date
RW-0001	Enriquecimiento y Contextualización de Origen	1	October 15, 2025	October 14, 2026
PEN-0001	Validación de Seguridad Automatizada	1	October 15, 2025	October 14, 2026
OA-0001	Observabilidad Avanzada	1	October 15, 2025	October 14, 2026
SIG-0001	Sistema Integral de Gestión de Riesgos y Cumplimiento	1	October 15, 2025	October 14, 2026

SOC Electoral 2025 > ENTREGABLES > 2. LICENCIAS

Nombre	Modificado	Modificado por
Licencias Mrevo Evolution IS.pdf	28 de octubre	James Gustavo Arana Reyes

MATRIZ DE RIESGOS

De acuerdo con la evaluación de Riesgos realizada al servicio IronShield, se identificaron nueve riesgos inherentes (9); los cuales son transversales a la operación SOC-CERT.

 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

Al analizarse los riesgos inherentes en el servicio; se establecieron tres (3) riesgos de tipo operativo y seis (6) riesgos de tipo de seguridad de la información.

El análisis de riesgos realizado al servicio tiene como objetivo principal identificar los riesgos inherentes del servicio; que de llegar a materializarse pueden afectar las actividades operativas y de seguridad de la información en el SOC-CERT. El análisis también contempla su clasificación de probabilidad, impacto y severidad; a saber, su nivel de riesgo. Se establece; de acuerdo con el análisis, que en términos de severidad se identificaron cuatro (4) riesgos en Extremo, tres (3) riesgos en Alto y dos (2) riesgos en Moderado. A continuación, se describe la Matriz de Riesgos Identificados.

No. DEL RIESGO	TIPO DE RIESGO	DESCRIPCIÓN DEL RIESGO	SERVICIO
R1	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 debido a deficiencias en la planificación y gestión del proyecto.	2 14 Servicio Iron Shield
R2	Operativo	Posibilidad de afectación económica y/o reputacional 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) debido a deficiencias en la gestión estratégica e incumplimiento de las funciones contractuales como líder SPMO	2 14 Servicio Iron Shield
R3	Seguridad de la información	Posibilidad de afectación económica, reputacional y legal por no identificar la infraestructura crítica cibernética y/o servicios esenciales debido a la entrega de información incompleta, desactualizada u omisión del cliente afectando la disponibilidad de la información	2 14 Servicio Iron Shield
R4	Operativo	Posibilidad de afectación económica por indisponibilidad de personal técnico y/o profesional idóneo en TIC - ciberseguridad para garantizar la continuidad de los servicios implementados en el SOC-CERT debido a retiro, desvinculación y/o rotación de personal	2 14 Servicio Iron Shield
R20	Seguridad de la información	Posibilidad de afectación económica, reputacional y legal por fuga, alteración, y/o acceso no autorizado de la información debido a errores en la configuración de roles o permisos para el acceso a la información afectando la confidencialidad de la información	2 14 Servicio Iron Shield
R21	Seguridad de la información	Posibilidad de afectación económica, reputacional y legal por error en la parametrización, actualización y/o mantenimiento de las diferentes plataformas tecnológicas (hardware y software) que soportan el servicio SOC-CERT debido a falta de gestión del servicio de infraestructura afectando la disponibilidad de la información	2 14 Servicio Iron Shield
R25	Seguridad de la información	Posibilidad de afectación económica, reputacional y legal por el uso de dispositivos portátiles corporativos sin hardening debido a la ausencia de controles de seguridad de la información afectando la confidencialidad, integridad o disponibilidad de la información	2 14 Servicio Iron Shield
R26	Seguridad de la información	Posibilidad de afectación económica y/o reputacional por no identificar e informar sobre eventos, alertas, amenazas, ciberamenazas, patrones y/o tendencias que afecten la infraestructura crítica, activos digitales y/o servicios esenciales del cliente debido a la falta de gestión efectiva de la información o ciclo de inteligencia afectando la integridad de la información	2 14 Servicio Iron Shield
R28	Seguridad de la información	Posibilidad de afectación económica, reputacional y legal por acceso no autorizado al ecosistema cibernético del SOC-CERT mediante dispositivos portátiles y/o de escritorio utilizados por colaboradores debido a la ausencia o inadecuada aplicación de políticas de control de acceso afectando la confidencialidad de la información	2 14 Servicio Iron Shield

SOC Electoral 2025 > ENTREGABLES > 3. RIESGOS

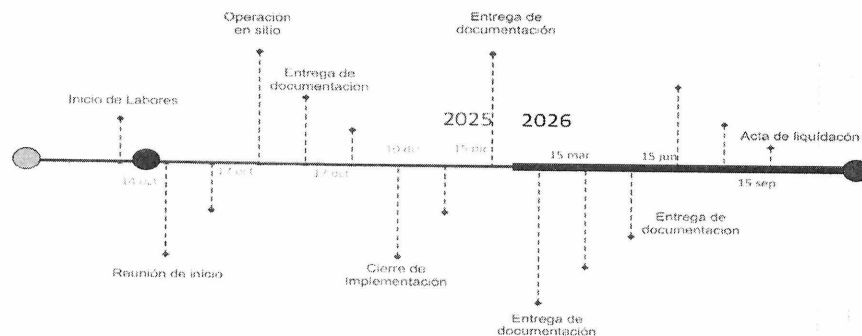
Nombre	Modificado	Modificado por
2.14 IDENTIFICACIÓN de Riesgos Servicio Escudo de Riesgo.xlsx	Hace 6 días	James Gustavo Arana Reyes
Identificación Riesgos Servicio Escudo de Hierro.pdf	28 de octubre	James Gustavo Arana Reyes
Matriz de Riesgo Servicio Escudo de Hierro.xlsx	28 de octubre	Juan Alberto Cardona Molina

 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

DIAGRAMA DE HITOS DEL PROYECTO

De acuerdo con la ejecución del presente contrato de presentación de servicio, se relaciona el diagrama de los hitos de este.



ENRIQUECIMIENTO Y CONTEXTUALIZACIÓN DE ORIGEN

Durante el periodo analizado se realizaron 5.358 consultas de diferentes indicadores de compromiso donde se puede evidenciar información de relevancia tales como: detalles de origen, score de riesgo, información avanzada de ataques, vectores de ataques usados, estas consultas permitieron integrar inteligencia proveniente de fuentes externas, OSINT y bases de datos de reputación para determinar el origen y características de los ataques, los que permite transformar los datos de ataques activos en información accionable para optimizar la detección y respuesta del SOC.

El servicio cuenta con suscripción activa de la plataforma de Enriquecimiento y contextualización de origen por la vigencia del contrato.

 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



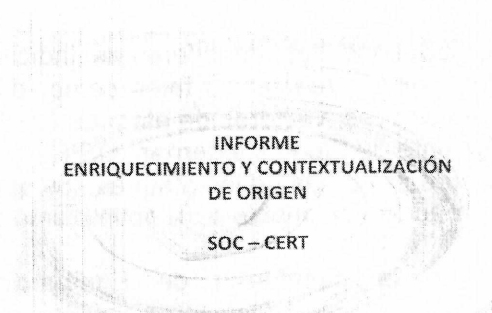
Threat Intelligence Center

Search Single IPv4 For Insight

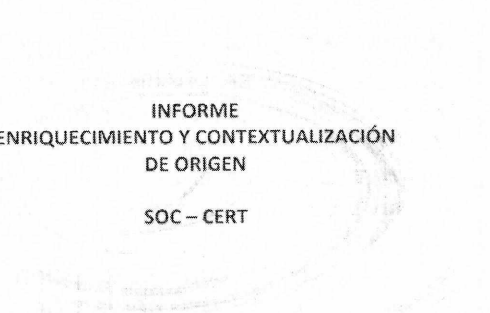
0005358 / 1.000.000 IP's were investigated so far this month

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

Nombre	Modificado	Modificado por
Analisis de origen 181025.pdf	28 de octubre	James Gustavo Arana Reyes
Analisis de origen 191025-6.pdf	28 de octubre	James Gustavo Arana Reyes
Archivo direcciones IP radiware OCTUBRE.xlsx	28 de octubre	James Gustavo Arana Reyes



INFORME
ENRIQUECIMIENTO Y CONTEXTUALIZACIÓN
DE ORIGEN
SOC – CERT



INFORME
ENRIQUECIMIENTO Y CONTEXTUALIZACIÓN
DE ORIGEN
SOC – CERT

Periodo del informe:

El presente documento, detalla el resumen y análisis obtenido de la gestión realizada sobre las soluciones de seguridad, para el cliente Registraduría Nacional del Estado Civil durante el siguiente periodo:

Fecha inicial de corte: 17/10/2025
Fecha final de corte: 19/10/2025

Periodo del informe:

El presente documento, detalla el resumen y análisis obtenido de la gestión realizada sobre las soluciones de seguridad, para el cliente Registraduría Nacional del Estado Civil durante el siguiente periodo:

Fecha inicial de corte: 15/10/2025
Fecha final de corte: 16/10/2025

 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

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
SALDO	\$ 40.814.893.058

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

SUPERVISOR



HOSLANDER ADLAI SÁENZ BARRERA
Gerente de Informática

Proyectó: Juan Alberto Cardona Molina
Revisó: Eduardo Emilio Calderón Narváez