

FRR Fondo Rotatorio 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 DE PRESTACIÓN DE SERVICIOS ELECTRÓNICO No 017 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:	Prestar servicios de mantenimiento y fortalecimiento del sistema de Gestión de Seguridad de la Información y ciberseguridad para la infraestructura tecnológica de la Entidad, de conformidad con el estudio previo, el anexo técnico y la propuesta presentada por EL CONTRATISTA, los cuales forman parte integral del contrato.
CIUDAD:	Bogotá
FECHA DE SUSCRIPCIÓN DEL CONTRATO:	14 de abril de 2025
FECHA DE INICIO:	15 de abril de 2025
FECHA DE TERMINACIÓN:	31 de mayo de 2026
INFORME NRO.	Adición Pago 2
PERIODO DE EJECUCIÓN:	01 al 28 de febrero 2026
FECHA PRESENTE INFORME:	2 de marzo de 2026

FRR Fondo Rotatorio 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

ACTIVIDADES

El 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. 017 de 2025, así como la ADICIÓN Y OTROSÍ No. 01 Y PRÓRROGA No. 02 al Contrato Interadministrativo electrónico N° 017 de 2025 -FRR con UNE EPM TELECOMUNICACIONES S.A. con sigla UNE TELCO, se desarrolló conforme lo establecido en Anexo Técnico y la CLÁUSULA TERCERA del Contrato, mediante la cual se estableció que para el séptimo pago, correspondiente al mes de febrero de 2026, avance del cronograma de las actividades descritas.

En esta sexta 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 mantenimiento y operación del sistema de Seguridad de la Información y Seguridad Cibernética para la Infraestructura Tecnológica de la Organización Electoral, asegurando el despliegue eficiente y puntual de los servicios acordados, a continuación, se describen los numerales supervisados:

MANTENIMIENTO Y OPERACIÓN DE LA PLATAFORMA TECNOLÓGICA Y LA ARQUITECTURA DE SEGURIDAD DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL - RNEC

La visión estratégica de seguridad ha sido desplegada e implementada en torno a cuatro grandes pilares: (1) un Comité estratégico, centralizado en la toma de decisiones en ciberseguridad para establecer medidas aplicables a los procesos de negocio actuales y futuros de la Registraduría Nacional, (2) un Servicio de seguridad, que Implementa servicios que abarcan la identificación, prevención, protección y respuesta ante incidentes y amenazas; tanto internas como externas, (3) una Gestión de crisis, que asegura una correcta recuperación y comunicación durante estados de emergencia y (4) un Ecosistema tecnológico integrado, que crea capacidades automáticas para la identificación temprana y la defensa adaptativa.

El comité Estratégico de Ciberseguridad está compuesto por personal experto de la Registraduría Nacional y profesionales del Centro de Operaciones de Seguridad SOC quienes tienen la responsabilidad de velar por la seguridad integral de los activos y son los responsables de evaluar tanto los nuevos proyectos de seguridad, como los sistemas e infraestructuras tecnológicas que se han implementado en la Registraduría Nacional, con la finalidad de identificar factores críticos que afecten a la seguridad y protección de los procesos de negocio, lo que ha permitido la integración en el modelo de seguridad actual, para aplicar todas las capacidades disponibles, haciéndolos integrantes del ecosistema de prevención y protección implementado a través del SOC-CERT.

De igual manera, fue implementada la Security Project Management Office (SPMO); la cual ha sido la responsable de gestionar y orquestar todos los servicios y procesos que se realizan en el Centro de Operaciones de Seguridad y están enclavados dentro de los "Servicios Gestionados de Seguridad", esta oficina ha tenido un control integral del estado de las

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

Aprobado:
06/06/2017

actividades que se están llevando a cabo a través del seguimiento diario de todas las actividades que conforman los diferentes servicios ofrecidos.

Así mismo, la SPMO se ha encargado de proveer a la Registraduría Nacional de valores únicos de seguridad que representan el nivel de riesgo actual del organismo en cada una de sus partes críticas y de ofrecer una visión unificada de las amenazas.

Por otra parte, la puesta en operación de la Seguridad Integral de las Elecciones se ha venido desarrollando una mejora al Framework denominado “360 Security Electoral Framework” que abarca la segmentación de los procesos electorales, el sistema de gobierno y control, el marco de controles, y las medidas estratégicas, operativas y tácticas para la seguridad y resiliencia de la infraestructura del proceso.

Este Framework se ha venido desarrollando a través de la implementación y despliegue de un “ECOSISTEMA DE SEGURIDAD E INTEGRIDAD PARA LAS ELECCIONES”, estableciendo un modelo de gobierno, gestión y control integral del proceso de seguridad y monitoreo, evaluación y defensa de los sistemas de información para proteger la confidencialidad, integridad y disponibilidad de los datos, antes, durante y después de los procesos electorales.

Las actividades se han potenciado en una Visión Global del Servicio que incluyen seis aspectos fundamentales:

1. El Comité Estratégico de Ciberseguridad está compuesto por personal experto de la Registraduría Nacional del Estado Civil y profesionales del Centro de Operaciones de Seguridad (SOC). Este comité tendrá la responsabilidad de velar por la seguridad integral de los activos, evaluando tanto los nuevos proyectos de seguridad como los sistemas e infraestructuras tecnológicas que se implementarán en la Registraduría Nacional del Estado Civil. Su objetivo será identificar factores críticos que afecten a la seguridad y protección de los procesos de negocio, facilitando la integración en el modelo de seguridad actual y aplicando todas las capacidades disponibles. Así, se integrarán en el ecosistema de prevención y protección implementado a través del SOC.
2. La Security Project Management Office (SPMO) es la unidad responsable de gestionar y coordinar todos los servicios y procesos del Centro de Operaciones de Seguridad. Los responsables de la SPMO tendrán un control integral del estado de las actividades mediante indicadores clave de rendimiento (KPIs) y cuadros de mando, lo que permitirá la toma de decisiones a nivel ejecutivo.
3. La Unidad de Corporate Security Intelligence es la responsable de modelar el ecosistema de la Registraduría Nacional del Estado Civil, abarcando sus principales activos humanos, físicos y tecnológicos, así como los principales procesos de negocio. Además, establecerá métricas para identificar en todo momento el nivel de exposición, amenaza y riesgo de impacto en cada uno de ellos.

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

Aprobado:
06/06/2017

Desde esta unidad se mantendrá la operación de servicios tales como, Global Risk Security Analysis (GRSA), Strategy Risk Analysis (SRA) y Cyber Research.

4. Dentro del pool de servicios brindados en la capa de SecureVisión donde la premisa son todas aquellas actividades que se enfocan en la detección, prevención y remediación frente a amenazas cibernéticas; para esto, se mantendrá la operación de los servicios con este enfoque, tales como las Auditorías Técnicas de Seguridad, la Gestión de Vulnerabilidades, la Threat Intelligence, entre otros.
5. Cybersecurity Event Monitoring mantiene y opera un sistema para unificar todo el conocimiento, facilitando su correcta gestión y explotación basada en algunas aplicaciones de inteligencia Artificial.
6. Cyber Incident Response permite la respuesta ante incidentes e implica que un grupo de expertos analice todos los eventos escalados como incidentes, realizando actividades como análisis forense, reversing de malware y análisis de tráfico. Este análisis permitirá el correcto modelado de la amenaza y el diseño de planes de tratamiento que definirán las pautas y acciones a seguir.
El equipo de respuesta a incidentes también será responsable de establecer y gestionar las acciones ante crisis, representando incidentes o amenazas con un impacto crítico para la Registraduría Nacional.

Para esto, se creará el mantenimiento y continuidad del servicio de monitorización de ciberseguridad, se integran todas las amenazas y vulnerabilidades descubiertas, junto con los logs de los sistemas críticos actuales, tanto operativos como de seguridad. Con esto, se realizan acciones esenciales para el mantenimiento y continuidad de la seguridad, entre ellas:

- Correlación de la información para el descubrimiento de amenazas avanzadas, identificación de patrones de comportamiento de riesgo, tanto de usuarios como de actores externos y de sistemas e infraestructuras.
- Diseño de casos de uso y defensas que automatizan la respuesta a los incidentes.

Para esto se adecuó una "War Room" operativa 24/7, donde los mejores expertos trabajarán en la gestión de la situación mediante el diseño de planes específicos estratégicos, operativos, tácticos y de comunicación.

En el presente informe se podrá identificar la implementación y despliegue realizado de cada uno de los servicios que conforman la Visión Global del Servicio, los cuales se encuentran soportados por una serie de soluciones tecnológicas que son permanentemente afinadas y monitoreadas por el Centro de Operaciones de Seguridad SOC de la Registraduría Nacional del Estado Civil, en aras de garantizar la continuidad de los servicios prestados a través de su infraestructura tecnológica en función de los procesos misionales.

FRR Fondo Rotatorio 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

MANTENIMIENTO Y OPERACIÓN DE LA PLATAFORMA TECNOLÓGICA Y LA ARQUITECTURA DE SEGURIDAD DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL - RNEC

Mediante la serie de servicios desplegados se ha podido garantizar un nivel de seguridad óptimo dentro del perímetro definido, enlazado con su plan de mejora de ciberseguridad, permitiéndole dotarse de una serie de procesos, herramientas y capacidades en esta área.

Con cada servicio se ha generado múltiples sinergias entre ellos, redundando en una mayor eficacia en la prestación y en la mejora de los niveles de seguridad de la entidad.

Con este modelo se ha podido:

- Garantizar la continuidad de los servicios prestados por la entidad.
- Mejorar la resolución de incidentes de seguridad y la capacidad de recuperación (resiliencia) frente a los mismos.
- Garantizar que existe un conjunto de procesos estables y maduros que faciliten la gestión y tratamiento de los incidentes.

Los servicios implementados y desplegados son:

Mantenimiento y operación del servicio Corporate Security Intelligence:

Este componente del servicio analiza la exposición y el riesgo digital de la organización para generar un indicador dinámico (KPI) que ha permitido monitorear en tiempo real el estado de la seguridad digital. Este índice multivectorial (Score) incluye los elementos clave que afectan al cliente, evaluando desde diversas perspectivas. Facilita la creación de planes estratégicos de acción en cada área para mejorar la madurez en seguridad.

El Score y su desglose pueden ser presentados en comités directivos para ilustrar el progreso de los planes estratégicos de mejora en la seguridad de la información y su impacto real.

Al ser un indicador dinámico, se realizó una evaluación periódica a medida que se implementaron las medidas de mejora, lo que permitió evaluar y demostrar su efectividad.

El servicio de Inteligencia de Seguridad Corporativa está orientado a la valoración del riesgo corporativo de la Entidad en el entorno digital, dando visibilidad estratégica de los principales tipos de ataques ciber criminales que recibe la Entidad; tanto desde la clear web, como desde la deep y Darknet.

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

Aprobado:
06/06/2017

Febrero 2026

Impact Score

Scoring	
A	91-100
B	81-90
C	71-80
D	61-70
E	51-60
F	≤ 50

Riesgo de exposición

2 /10

Principales amenazas

- Filtraciones de credenciales en descenso
- Movilizaciones sociales cerca de la sede de RNEC
- Aumento de las alertas reputacionales

Riesgo técnico

5 /10

Principales amenazas

- Protocolo TLS/SSL inseguro en activo crítico
- CSP ausente
- No se implementan las mejores prácticas X-Content-Type-Options

Se adjunta: FEBRERO

> 2. SERVICIOS > 2.01 CORPORATE SE... > 02- FEBRERO 2026

Compartir Copiar vínculo Agregar acceso directo a OneDrive Descargar

Todos los documentos + Agregar vista

Nombre	Modificado	Modificado por	Creado	Creado por
[RNEC] Informe de seguimiento_Registrador_Registraduría_27.02.2026.pdf	Hace unos segundos	Yenny Fernanda Hern	Hace unos segundos	Yenny Fernanda Hernandez Perez
[RNEC] Informe de seguimiento_Registrador_Registraduría_26.02.2026.pdf	Ayer a las 8:16	Yenny Fernanda Hern	Ayer a las 8:16	Yenny Fernanda Hernandez Perez
[RNEC] Informe de seguimiento_RegistradorNacional_25.02.2026.pdf	Ayer a las 8:18	Yenny Fernanda Hern	Ayer a las 8:18	Yenny Fernanda Hernandez Perez
[RNEC] Informe de seguimiento_RNEC_25.02.2026.pdf	Ayer a las 8:18	Yenny Fernanda Hern	Ayer a las 8:18	Yenny Fernanda Hernandez Perez
[RNEC] Informe de seguimiento_Elecciones Congreso 2026.pptx.pdf	Ayer a las 8:55	Yenny Fernanda Hern	Ayer a las 8:55	Yenny Fernanda Hernandez Perez
[RNEC] Informe mensual reputacional_Enero-Febrero_2026.pptx.pdf	Ayer a las 8:56	Yenny Fernanda Hern	Ayer a las 8:56	Yenny Fernanda Hernandez Perez
2.1. Mantenimiento y operación del servicio Inteligencia de Seguridad Corporativa.pdf	Hace 6 días	Yenny Fernanda Hern	Hace 6 días	Yenny Fernanda Hernandez Perez

- Informe GRSA: Este componente del servicio analiza la exposición y el riesgo digital de la organización para generar un indicador dinámico (KPI) que permita monitorear en tiempo real el estado de la seguridad digital.

Se adjunta: FEBRERO

> 2.01 CORPORATE SE... > GRSA - GLOBAL RIS... > 02. FEBRERO 2026

Compartir Copiar vínculo Agregar acceso directo a OneDrive Descargar

Todos los documentos + Agregar vista

Nombre	Modificado	Modificado por	Creado	Creado por
[RNEC][GRSA] 2. Informe Mensual Febrero.pdf	Hace unos segundos	Yenny Fernanda Hern	Hace 9 días	Yenny Fernanda Hernandez Perez

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

Aprobado:
06/06/2017

- Informe SRA: Este servicio permite contar con una perspectiva estratégica y dinámica del riesgo corporativo en el ámbito digital.

Se adjunta: SRA

2. SERVICIOS > 2.01 CORPORATE SE... > SRA - STRATEGY RIS... > 2026

Compartir Copiar vínculo Agregar acceso directo a OneDrive Descargar

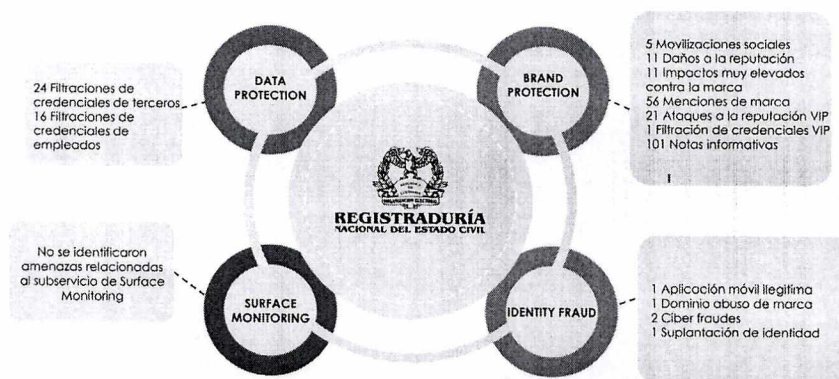
Cambiar no guardados

Todos los documentos + Agregar vista

Nombre	Modificado	Modificado por	Creado	Creado por
SRA 2. Informe Mensual Febrero 2026.pdf	Hace 6 días	Yenny Fernanda Hern	Hace 6 días	Yenny Fernanda Hernandez Perez

Mantenimiento y operación del servicio Vigilancia Digital & Cyber Threat Intelligence para la de seguridad de la Registraduría Nacional del Estado Civil y los procesos electorales:

El despliegue y puesta en marcha del servicio de Vigilancia Digital permitió a la Registraduría Nacional del Estado Civil ejecutar con los procesos de identificación y seguimiento de posibles amenazas y/o incidentes concretos de ciberseguridad que se originan en los entornos digitales de internet pública y la denominada "internet profunda", como una estrategia efectiva para anticipar posibles acciones que pueden afectar los intereses de la Registraduría Nacional del Estado Civil.



Se adjunta: FEBRERO

2.02 VIGILANCIA DI... > VIGILANCIA DIGITAL > 02. FEBRERO 2026

Compartir Copiar vínculo Agregar acceso directo a OneDrive Descargar + Crear o cargar

Todos los documentos + Agregar vista

Nombre	Modificado	Modificado por	Creado	Creado por
[RNEC] Informe de seguimiento_Elecciones Congreso 2026.pdf	El martes a las 10:30	James Gustavo Arana	El martes a las 10:30	James Gustavo Arana Reyes
2.2.1 Vigilancia Digital.pdf	21 de febrero	Yenny Fernanda Hern	21 de febrero	Yenny Fernanda Hernandez Perez

FRR Fondo Rotatorio 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

En el despliegue y puesta en marcha del servicio de Cyber Threat Intelligence se mantuvo el enriquecimiento de información a la Registraduría Nacional del Estado Civil, sobre aquellas amenazas que pueden materializar algún evento de Seguridad, con esto, se logrará:

- Identificación y parametrización de los activos a monitorizar.
- Monitorización y selección de las amenazas que afectan a la Registraduría Nacional del Estado Civil en sus diferentes filiales, geografías y sectores.
- Generación de alertas de incidentes en caso de detección de fuga de datos, exposición de credenciales o manipulación de dominios asociados a la marca de la Registraduría Nacional del Estado Civil.
- Análisis de las amenazas más complejas y de la totalidad de las amenazas identificadas para mejor el entendimiento del panorama de seguridad.
- Priorización de las amenazas de mayor riesgo (impacto + probabilidad) hacia Registraduría Nacional del Estado Civil y sus actividades.
- Evaluación geográfica y sectorial del panorama de amenazas para mejor la comprensión del posicionamiento de la Registraduría Nacional del Estado Civil en términos de ciberseguridad con respecto a la competencia.
- Mediante la operación del servicio de Cyber Threat Intelligence se desarrollaron las actividades de alertas preventivas, donde se articularon el conocimiento generado a través de los analistas de seguridad y la inteligencia para la reducción de riesgos relacionados con la seguridad TI y prevención en la exposición ante amenazas y ataques.

Se adjunta: FEBRERO

> 2. SERVICIOS > 2.02 VIGILANCIA DI... > CTI > 02. FEBRERO 2026				Compartir	Copiar vínculo	Agregar acceso directo a OneDrive	Descargar	+ Crear o cargar
Todos los documentos + Agregar vista				Detalles				
Nombre	Modificado	Modificado por	Creado	Creado por				
2.2.2. Mantenimiento y operación del servicio Cyber Threat Intelligence.pdf	21 de febrero	Yenny Fernanda Heltz	21 de febrero	Yenny Fernanda Hernandez Perez				

Auditorías Técnicas de Seguridad para la Registraduría Nacional del Estado Civil y los procesos electorales:

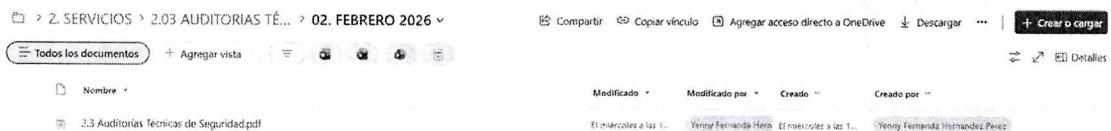
El objetivo de dar continuidad a este servicio es seguir recopilando y verificando todas las posibles amenazas de seguridad a las que está expuesta la infraestructura tecnológica de la Registraduría Nacional del Estado Civil. Para ello, se continuará la identificación y explotación de vulnerabilidades en los diversos activos y entornos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información corporativa, así como afectar la imagen de la Registraduría Nacional del Estado Civil. Para ello, se emplean técnicas avanzadas para detectar, reportar y establecer contramedidas que reduzcan la exposición; tanto a nivel externo como interno.

FRR Fondo Rotatorio 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

Con base a los resultados obtenidos, se generaron recomendaciones que aportan un valor diferenciador a la Registraduría Nacional del Estado Civil mediante pruebas altamente cualificadas y un análisis profundo de los resultados. De esta manera, se proporcionó información sobre el riesgo o impacto real en el que se encuentra la organización y las medidas recomendadas para disminuir dicho riesgo a niveles aceptables.

Se adjunta: FEBRERO

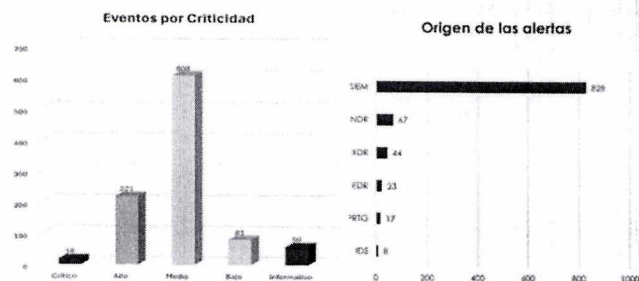


Mantenimiento y operación del servicio de Monitorización de Eventos de Seguridad para la Registraduría Nacional del Estado Civil y los procesos Electorales:

El servicio de Monitorización de Eventos mantiene una visión holística que incluye la detección y tratamiento de eventos, identificando de un modo ágil y eficiente los incidentes de seguridad a ser tratados; para esto, se opera el servicio desde un marco de trabajo que contempla el ciclo completo de monitorización y la gestión de incidentes, donde se incluyen las fases de detección, análisis y soporte de contención para los incidentes de seguridad.

El servicio de monitorización de eventos mantiene los procedimientos correspondientes que responden de manera eficiente a las necesidades y características de los sistemas tecnológicos de la información pertenecientes a la Registraduría Nacional del Estado Civil, los mecanismos procedimentales que mantienen la operación están operados por personal calificado, realizando las labores de monitorización permanente 24/7 por el tiempo contrato.

Se ha seleccionado como SIEM el producto IBM Security QRadar, del fabricante IBM, por su posicionamiento en cuanto a capacidades frente a otros fabricantes. Qradar permite su integración completa con las herramientas de tecnologías de la información y cubre ampliamente las necesidades de potencia de correlación necesaria para la infraestructura planteada en el pliego. La infraestructura de correlación permite la modalidad de Alta Disponibilidad, dada su criticidad en la solución propuesta.



FRR Fondo Rotatorio 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

Se adjunta: FEBRERO

2. SERVICIOS > 2.04 MONITORIZACI... > 02. FEBRERO 2026

Compartir Copiar vínculo Agregar acceso directo a OneDrive Descargar + Crear o cargar

Todos los documentos + Agregar vista

Nombre	Modificado	Modificado por	Creado	Creado por
2.4. Informe mensual de Monitorización Febrero 2026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
2.4. Mantenimiento y operación del servicio de Monitorización de Eventos de Seguridad.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez

- 5 Playbooks de casos de uso.

Se adjunta: PLAYBOOKS

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.04 MONITORIZACIÓN DE EVENTOS DE SE... > CASOS DE USO

Camión no guardados

Todos los documentos + Agregar vista

Nombre	Modificado	Modificado p...	Creado	Creado por
CASO DE USO Y PLAYBOOK - ASYNCRAT IOC DETECTOR.pdf	Hace un minuto	Yenny Fernanda Her...	Hace un minuto	Yenny Fernanda Hernandez Perez
CASO DE USO Y PLAYBOOK - CTI Windows-MALWARE DETECTION DCRat Trojan.pdf	Hace un minuto	Yenny Fernanda Her...	Hace un minuto	Yenny Fernanda Hernandez Perez
CASO DE USO Y PLAYBOOK - BAT-EXECUTION-SY-ASYNCRAT.pdf	Hace un minuto	Yenny Fernanda Her...	Hace un minuto	Yenny Fernanda Hernandez Perez
CASO DE USO Y PLAYBOOK - CTI IOC THREATQ ANALYSIS.pdf	Hace un minuto	Yenny Fernanda Her...	Hace un minuto	Yenny Fernanda Hernandez Perez
CASO DE USO Y PLAYBOOK - CTI Windows FILE WSF INITIAL PHASE-NIRAT.pdf	Hace un minuto	Yenny Fernanda Her...	Hace un minuto	Yenny Fernanda Hernandez Perez

- 28 informes diarios de la Operación SOC:

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.04 MONITORIZACIÓN DE EVENTOS DE SE... > INFORMES DIARIOS > 2026 > 2. FEBRERO 2026

Camión no guardados

Todos los documentos + Agregar vista

Nombre	Modificado	Modificado p...	Creado	Creado por
Informe Diario TIGO 28022026.pdf	Hace unos segundos	Yenny Fernanda Her...	Hace unos segundos	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 27022026.pdf	Hace unos segundos	Yenny Fernanda Her...	Hace unos segundos	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 26022026.pdf	Hace unos segundos	Yenny Fernanda Her...	Hace unos segundos	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 25022026.pdf	Hace unos segundos	Yenny Fernanda Her...	Hace unos segundos	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 24022026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 23022026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 22022026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 21022026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 21022026 Informe diario Segundo Simulacro Fecontes.pdf	22 de febrero	James Gustavo Ariza	22 de febrero	James Gustavo Ariza Reyes
Informe Diario TIGO 20022026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 19022026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 18022026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 17022026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 16022026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 15022026.pdf	El miércoles a las 1...	Yenny Fernanda Her...	El miércoles a las 1...	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 14022026.pdf	16 de febrero	Yenny Fernanda Her...	16 de febrero	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 13022026.pdf	16 de febrero	Yenny Fernanda Her...	16 de febrero	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 12022026.pdf	16 de febrero	Yenny Fernanda Her...	16 de febrero	Yenny Fernanda Hernandez Perez
Informe Diario TIGO 11022026.pdf	16 de febrero	Yenny Fernanda Her...	16 de febrero	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

FRR Fondo Rotatorio 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 informes semanales:
- Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.04 MONITORIZACIÓN DE EVENTOS DE SE... > INFORMES SEMANALES > 2026 > 02. FEBRERO 2026 >

Cambiar vista: [Todos los documentos](#) + Agregar vista

Nombre	Modificado	Modificado por	Creado	Creado por
Informe semanal: 45 del 16 de febrero al 22 de febrero 2026.pdf	Hace un minuto	Tenny Farnanda Harnan	Hace un minuto	Tenny Farnanda Harnan
Informe semanal: 44 del 09 de febrero al 15 de febrero 2026.pdf	El miércoles a las 1...	Tenny Farnanda Harnan	El miércoles a las 1...	Tenny Farnanda Harnan
Informe semanal: 43 del 02 de febrero al 08 de febrero 2026.pdf	18 de febrero	Tenny Farnanda Harnan	19 de febrero	Tenny Farnanda Harnan

Mantenimiento y operación del servicio de Respuesta a Incidentes:

El principal objetivo referente a la continuidad del servicio de Respuesta a Incidentes es brindar a la Registraduría Nacional del Estado Civil, la certeza de continuar con los procesos de detección, el análisis y la contención del incidente a través del equipo de Threat Intelligence.

Cuando un evento es catalogado como incidente, el servicio de Respuesta a Incidentes procede a ejecutar las actividades requeridas para dar una pronta gestión a la respuesta frente al incidente, para ello; el SOC cuenta con los medios, mecanismos, procedimiento y tecnologías para realizar la detección, evaluación y acción frente a cualquier situación de incidente cibernético. A través de esto, los objetivos principales de este servicio se enmarcan en:

- Controlar y minimizar cualquier tipo de daño a la organización y su información, junto con la preservación de evidencias sobre lo ocurrido y la documentación correspondiente. De esta forma, se conocerá el contexto del incidente, que permitirá determinar su origen y posibles consecuencias.
- Coordinar las actividades para una recuperación rápida y eficiente de los sistemas y servicios que se hayan visto afectados, en conjunto con los equipos de tecnologías de la información, de manera que la organización pueda operar con normalidad en el menor tiempo posible y con el menor impacto tolerable.
- Investigar y erradicar las causas raíz del incidente, así como establecer las medidas oportunas para prevenir que eventos similares puedan ocurrir en el futuro.
- En caso necesario, se gestiona un Comité de Crisis para realizar la gestión de la misma y la toma de decisiones urgentes en función de la gravedad del incidente, siempre en coordinación con Registraduría Nacional.

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.05 RESPUESTA A INCIDENTES > 02. FEBRERO 2026 >

Cambiar vista: [Todos los documentos](#) + Agregar vista

Nombre	Modificado	Modificado por	Creado	Creado por
Quemados DLP	18 de febrero	Josely Guzmán Araya	19 de febrero	Josely Guzmán Araya
SQL Injection UT	19 de febrero	Josely Guzmán Araya	19 de febrero	Josely Guzmán Araya
Alcance análisis archivo en: 001_Notificacion_Oficial_Jurado_200212962026_exec.pdf	El jueves a las 6:25	Josely Guzmán Araya	El jueves a las 6:25	Josely Guzmán Araya
2.5. Mantenimiento y operación del servicio de Respuesta a Incidentes.pdf	El jueves a las 18:30	Tenny Farnanda Harnan	El jueves a las 18:30	Tenny Farnanda Harnan

FRR Fondo Rotatorio 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

Mantenimiento y operación del servicio de Gestión de Crisis de Seguridad para la Registraduría Nacional del Estado Civil y los procesos electorales:

El objetivo de esta línea de servicios es continuar reforzando, entrenando y apoyando bajo demanda en las capacidades, protocolos y responsabilidades que permitan anticipar y responder de manera ágil a las ciberamenazas de mayor severidad y complejidad creciente que afecten a los activos de la Registraduría Nacional del Estado Civil. Para estas labores se cuenta con laboratorios especializados y la amplia experiencia acumulada por nuestros analistas de inteligencia de ciberamenazas; quienes son capaces de anticipar y entender las campañas de ciberdelinquentes, entrenarlas y gestionar su impacto desde las perspectivas operativa, legal (forense) y organizativa.

El plan de gestión de crisis contempla la preparación, detección y gestión de cualquier incidente de origen tecnológico cuyo impacto sea transversal a la Entidad, tenga cierta repercusión externa y cuya vía de resolución sea incierta, teniendo en cuenta:

- El modelo organizativo más adecuado, por niveles y ámbitos de competencia, para abordar el ciclo de vida completo de una crisis de origen cibernético.
- El modelo de seguimiento y reporte adecuado de la crisis desde su detección hasta su cierre.
- Criterios de escalado entre niveles de alerta a raíz de los indicadores que desde sistemas pueden medirse.
- Recursos y tecnología de apoyo para una gestión eficiente del ciclo de vida de la crisis.

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.06 GESTIÓN DE CRISIS DE SEGURIDAD > 02. FEBRERO 2026 >

Todos los documentos	+ Agregar vista						
Nombre	Modificado	Modificado por	Creado	Creado por			
2.6. Mantenimiento y operación del servicio de Gestión de Crisis.pdf	Hace unos segundos	Yenny Fernanda Herra	Hace unos segundos	Yenny Fernanda Hernandez Diaz			

Mantenimiento y operación del servicio Threat Hunting:

El objetivo principal es dar continuidad al servicio de Threat Hunting actuando de manera proactiva en la infraestructura de la Registraduría Nacional del Estado Civil para identificar amenazas que no han sido detectadas por las soluciones actuales. Además, siguiendo con la identificación de incidentes que ya han ocurrido en la infraestructura y de los cuales no se tenía conocimiento.

Basándose en misiones de hunting, los analistas priorizarán la búsqueda de amenazas según las técnicas más frecuentemente utilizadas por los cibercriminales, de acuerdo con las estadísticas. Gracias a este modelo de trabajo, se cubrirán técnicas basadas en la matriz

FRR Fondo Rotatorio 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

ATT&CK de MITRE, permitiendo enfocar los esfuerzos en aquellas que no se han implementado y sobre las que se desarrollan las principales actividades.

Cada misión de hunting completada se automatizará en formato de "identificación preventiva", permitiendo que los analistas se concentren en nuevas misiones y evitando la pérdida de tiempo en detectar comportamientos pasados, ya que estos serán identificados automáticamente.

Continuar con este modelo de trabajo permitirá que la Registraduría Nacional del Estado Civil, con el tiempo, siga cubriendo una gran cantidad de técnicas de intrusiones por los principales grupos de cibercriminales. Esto permitirá seguir facilitando la automatización y el enfoque en las nuevas técnicas que vayan descubriéndose, enriqueciendo indirectamente otros servicios ofertados.

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.07 THREAT HUNTING > 02. FEBRERO 2026 ~

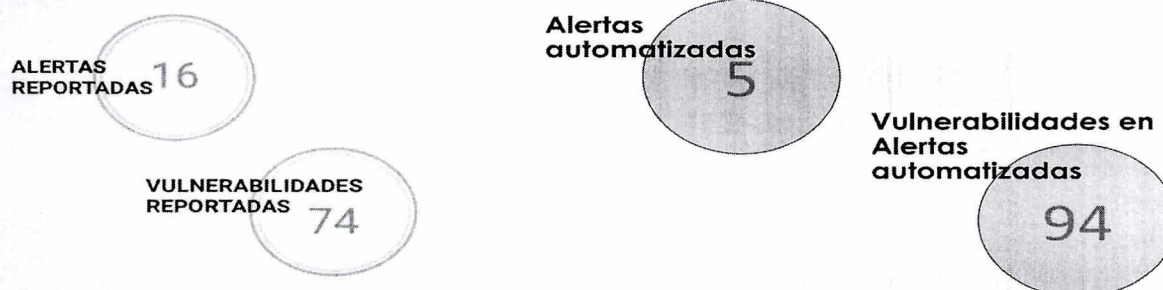
Todos los documentos + Agregar vista		Nombre	Modificado	Modificado p...	Creado	Creado por
		2.7. Mantenimiento y operación del servicio Threat Hunting.pdf	21 de febrero	Yenny Fernanda Herra	21 de febrero	Yenny Fernanda Hernández Pérez

Mantenimiento y operación del servicio Alerta Temprana:

Mediante la continuidad operativa del servicio de Alerta Temprana se articula el conocimiento generado a través de los analistas de seguridad y de inteligencia para la reducción de riesgos relacionados con la seguridad tecnologías de la información y prevención en la exposición ante amenazas y ataques.

El servicio de Alerta Temprana articula el conocimiento de los activos de la Registraduría Nacional del Estado Civil e identifica vulnerabilidades que puedan afectar los activos o software.

El alertamiento temprano describe de manera precisa; tanto las vulnerabilidades a las cuales se puedan ver expuestos los sistemas informáticos, cómo el conjunto de acciones y relaciones entre los actores y las responsabilidades que deberán asumir y ejecutar cada uno de ellos.



FRR Fondo Rotatorio 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 adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.08 ALERTA TEMPRANA > 02. FEBRERO 2026 ~

Todos los documentos + Agregar vista

Nombre

Modificado

Modificado p...

Creado

Creado por

2.6. Mantenimiento y operación del servicio Alerta Temprana.pdf

21 de febrero

Nancy Fernanda Herra 21 de febrero

Nancy Fernanda Herra Herra Rincón

Mantenimiento y operación del servicio Alerta Preventiva:

Mediante la continuidad del servicio de Alerta Preventiva se desarrollan actividades de alertas preventivas donde se articula el conocimiento generado a través de los analistas de seguridad y de inteligencia para la reducción de riesgos relacionados con la seguridad de tecnologías de la información y prevención en la exposición ante amenazas y ataques.

Las alertas preventivas permiten contar con información organizada en tres grandes ámbitos clave. El equipo del SOC continuará generando periódicamente este tipo de alertas para anticiparse a riesgos emergentes y fortalecer la postura de seguridad de la organización.

- **Ámbito sectorial:** Este ámbito tiene como objetivo alertar sobre eventos, ataques ocultos o campañas que atenten contra la seguridad informática de sectores específicos, como el financiero, energético, de comunicaciones, entre otros. Ofrece una visión general del estado del sector y de sus principales amenazas. A cada cliente se le asigna un sector en función de su actividad principal, lo que permite una mayor precisión en la contextualización de los riesgos.
- **Ámbito de inteligencia:** Se orienta a la identificación de eventos relacionados con tendencias de ataque, campañas avanzadas (APT) y actores ocultos que son detectados a través de herramientas automatizadas y analistas especializados en inteligencia. Este tipo de alertas se considera altamente relevante, ya que proporciona información anticipada sobre amenazas externas desconocidas, con alto nivel de sofisticación y capacidad de materialización.
- **Ámbito de alertas globales:** Está centrado en advertir sobre eventos de seguridad que pueden afectar indirectamente a la organización. Se evalúan las principales amenazas globales que están impactando a los medios de tecnologías de la información y el equipo del SOC analiza el potencial de que estas amenazas se materialicen, notificando al cliente si se determina que podrían afectar su infraestructura o activos críticos.

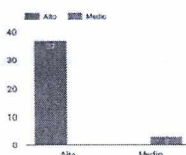
Se generan 40 alertas y eventos MISP durante el periodo reportado
Alertas y eventos MISP reportados

40

Se generan 2 reporte de actividad durante el periodo reportado
REPORT ACTIVITY

2

Se muestra la criticidad de las alertas generadas durante el periodo reportado



Se reportan 9.357 indicadores de compromiso con respecto a las amenazas analizadas

IoC Reportados

9.357

Se reportan 16 actores de amenaza involucrados con respecto a las alertas enviadas.

Actores maliciosos reportados

16

FRR Fondo Rotatorio 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 adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.09 ALERTA PREVENTIVA > 02. FEBRERO 2026

Todos los documentos	+ Agregar vista				
Nombre	Modificado	Modificado p...	Creado	Creado por	
2.9 Mantenimiento y operación del servicio Alerta Preventiva.pdf	21 de febrero	Yenny Fernanda Herra	21 de febrero	Yenny Fernanda Hernandez Perez	

Servicio Protección de Prestigio

El Servicio de Protección de Prestigio ofrece una solución integral para la detección, análisis y protección contra amenazas en línea, mediante el uso de una red global de sondas, inteligencia artificial (IA), procesamiento de lenguaje natural (NLP) y técnicas avanzadas de machine learning. El servicio monitorea internet desde la fuente de generación de contenido, proporcionando protección mediante el descubrimiento e inspección de amenazas, así como la identificación de campañas, actores y redes de bots.

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.10 PROTECCIÓN DE PRESTIGIO > 02. FEBRERO 2026

Todos los documentos	+ Agregar vista				
Nombre	Modificado	Modificado p...	Creado	Creado por	
2.10 Protección de Prestigio.pdf	21 de febrero	Yenny Fernanda Herra	21 de febrero	Yenny Fernanda Hernandez Perez	

Servicio Avanzado de Análisis, visibilidad y Respuesta Basado en el contexto de compromiso para la detección de amenazas.

El Servicio avanzado de análisis, visibilidad y respuesta basado en el contexto de compromiso para la detección de amenazas en endopints y servidores por medio del análisis de eventos en múltiples capas, identificando patrones anómalos en los procesos y finalizando aquellos sospechosos antes de que causen daños.

El servicio realiza la evaluación del impacto generado por un ataque dirigido, proporcionando detalles sobre su origen y progresión, y permita planificar una estrategia efectiva de respuesta ante incidentes de seguridad, realizando análisis iniciales para identificar endpoints que requieran un examen detallado.

Se adjunta: 02. FEBRERO 2026

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.11 DETECCIÓN DE AMENAZAS > 2.11.1 DETECCIÓN DE ATAQUES > 02. FEBRERO 2026

Todos los documentos	+ Agregar vista				
Nombre	Modificado	Modificado p...	Creado	Creado por	
2.11.1. Servicio para la detección de ataques en el Endpoint y servidores.pdf	El miércoles a las 7	Yenny Fernanda Herra	El miércoles a las 1...	Yenny Fernanda Hernandez Perez	

FRR Fondo Rotatorio 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

Se adjunta: 02. FEBRERO 2026

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.11 DETECCIÓN DE AMENAZAS > 2.11.2 DESCUBRIMIENTO DE AMENAZAS > 02. FEBRERO 2026 >

Todos los documentos	+ Agregar vista				
Nombre	Modificado	Modificado por	Creado	Creado por	
2.11.2. Servicio para el descubrimiento de amenazas a través del análisis del metadato.pdf	El miércoles a las 11...	Nancy Fernández Pérez	El miércoles a las 11...	Nancy Fernández Hernández Pérez	

Gestión de la Respuesta ante la identificación y remediación de Vulnerabilidades en la plataforma tecnológica.

El servicio de Monitorización de vulnerabilidades tiene como función principal realizar la identificación, evaluación y priorización de vulnerabilidades en la infraestructura tecnológica de la organización. A través de los hallazgos se definen acciones y planes de remediación, los cuales fortalecen la postura de seguridad de la organización.

Durante este periodo de evaluación del servicio, en el informe entregado se detallan los avances del servicio, los entregables, el comportamiento del servicio, los riesgos y recomendaciones. Como parte del servicio de Gestión de Vulnerabilidades, se realiza una evaluación continua de la ciber-exposición, herramienta líder en análisis de vulnerabilidades y gestión de riesgos de seguridad. Esta evaluación permite a la Entidad medir, visualizar y reducir su superficie de ataque, entendiendo de manera precisa qué tan expuestos están sus activos tecnológicos ante amenazas explotables.

El Cálculo del Cyber Exposure Score (CES), es un indicador cuantitativo que resume el nivel de exposición de la organización y permite compararlo en el tiempo o contra benchmarks del sector.

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.12 GESTIÓN DE LA RESPUESTA DE VULNERAB... > 2026 > 02. FEBRERO 2026

Todos los documentos	+ Agregar vista				
Nombre	Modificado	Modificado por	Creado	Creado por	
2.12 Informe del Servicio - Monitorización de Vulnerabilidades.pdf	El miércoles a las 11...	Nancy Fernández Pérez	El miércoles a las 11...	Nancy Fernández Hernández Pérez	
Informe de Vulnerabilidades - Febrero 2026.pdf	El miércoles a las 11...	Nancy Fernández Pérez	El miércoles a las 11...	Nancy Fernández Hernández Pérez	

- 26 Actas de seguimiento de la gestión de vulnerabilidades:

Se adjunta: Actas

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.12 GESTIÓN DE LA RESPUESTA DE VULNERAB... > ACTAS >

Todos los documentos	+ Agregar vista				
Nombre	Modificado	Modificado por	Creado	Creado por	
026. Acta Reunion Vulnerabilidades - 04/02/2024.pdf	Hoy a las 10:00	Nancy Fernández Pérez	Hoy a las 10:00	Nancy Fernández Hernández Pérez	
025. Acta Reunion Vulnerabilidades - 28/12/2023.pdf	3 de febrero	Nancy Fernández Pérez	3 de febrero	Nancy Fernández Hernández Pérez	
024. Acta Reunion Vulnerabilidades - 09/10/2023.pdf	10/10/2023	Nancy Fernández Pérez	10/10/2023	Nancy Fernández Hernández Pérez	
023. Acta Reunion Vulnerabilidades - 28/12/2023.pdf	11/12/2023	James Guisao Arias Rojas	11/12/2023	James Guisao Arias Rojas	
022. Acta Reunion Vulnerabilidades - 25/10/2023.pdf	11/12/2023	James Guisao Arias Rojas	11/12/2023	James Guisao Arias Rojas	
021. Acta Reunion Vulnerabilidades - 05/10/2023.pdf	12/12/2023	Nancy Fernández Pérez	11/12/2023	James Guisao Arias Rojas	
020. Acta Reunion Vulnerabilidades - 04/10/2023.pdf	10/12/2023	Nancy Fernández Pérez	10/12/2023	James Guisao Arias Rojas	
019. Acta Reunion Vulnerabilidades - 21/02/2023.pdf	12/12/2023	Nancy Fernández Pérez	11/12/2023	James Guisao Arias Rojas	
018. Acta Reunion Vulnerabilidades - 16/02/2023.pdf	10/12/2023	Nancy Fernández Pérez	11/12/2023	James Guisao Arias Rojas	
017. Acta Reunion Vulnerabilidades - 09/02/2023.pdf	10/12/2023	Nancy Fernández Pérez	11/12/2023	James Guisao Arias Rojas	

Gerencia de Informática

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

www.registraduria.gov.co

Se adjunta: WEB

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.12 GESTIÓN DE LA RESPUESTA DE VULNERAB...

Compartir Copiar vínculo Eliminar Favorito Agregar acceso directo a OneDrive Descargar Mover a Copiar en Editar en vista de cuadrícula Cambiar nombre Automatizar ...

Nombre

Modificado Modificado p... Creado Creado por

068.WAS_CLO_2026-02-11 Portalppi

El jueves a las 16:07 James Gustavo Arana El jueves a las 16:07 James Gustavo Arana Reyes

Se adjunta: INFRAESTRUCTURA

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.12 GESTIÓN DE LA RESPUESTA DE VULNERAB... > INFRAESTRUCTURA

Compartir Copiar vínculo Eliminar Favorito Agregar acceso directo a OneDrive Descargar Mover a Copiar en Editar en vista de cuadrícula Cambiar nombre Automatizar ...

Nombre

Modificado Modificado p... Creado Creado por

094.VM2_LOC_2026-02-12_WindowsAvanzado

El jueves a las 15:59 James Gustavo Arana El jueves a las 15:59 James Gustavo Arana Reyes

093.VM2_LOC_2026-02-13 Linux Avanzado

El jueves a las 16:07 James Gustavo Arana El jueves a las 16:07 James Gustavo Arana Reyes

083.VM2_LOC_2026-01-28 alpicap01022026

El jueves a las 16:04 James Gustavo Arana El jueves a las 16:04 James Gustavo Arana Reyes

Servicios para la atención de eventos de y para la infraestructura tecnológica basadas en las mejores prácticas de ITIL.

El servicio para la atención de eventos de la infraestructura tecnológica tiene como propósito garantizar la gestión oportuna, controlada y trazable de peticiones e incidencias, mediante la operación de un Modelo de Gestión de Servicios (SPMO) alineado con las mejores prácticas de ITIL V4. Este servicio se basa en la aplicación de prácticas que integran recursos organizacionales, capacidades operativas y soluciones tecnológicas para asegurar la continuidad, calidad y eficiencia en la prestación del servicio. A través de la práctica de Gestión de Peticiones e Incidencias, el servicio establece un flujo estructurado que comprende la notificación, el registro, la priorización, la ejecución, la validación y el cierre de cada solicitud o incidente, garantizando la asignación de responsables, el cumplimiento de los acuerdos de niveles de servicio (SLA), la evaluación de cargas de trabajo y la entrega de resultados verificables. De esta manera, el servicio contribuye a fortalecer la gobernanza operativa, la experiencia del usuario y la mejora continua en la gestión de la infraestructura tecnológica.

Se adjunta: 02. FEBRERO 2026



Infraestructura

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.13 ATENCIÓN DE EVENTOS DE Y PARA LA INF... > 02. FEBRERO 2026

Todos los documentos + Agregar vista

Nombre

Modificado Modificado p... Creado Creado por

2.13 Servicio Atención de Eventos de y para la Infraestructura Tecnológica Basada en Mejores Prácticas ITIL...

El miércoles a las 2... Yenny Fernanda Nieto El miércoles a las 2... Yenny Fernanda Hernández Pérez

FRR Fondo Rotatorio 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

Generar un conjunto de herramientas mediante la creación de dominios que faciliten el seguimiento del marco de control asociado a políticas y normativas aplicables.

El servicio de "Generar un conjunto de herramientas mediante la creación de dominios que faciliten el seguimiento del marco de control asociado a políticas y normativas aplicable" constituye el núcleo operativo para el fortalecimiento del Framework Electoral de Colombia. Bajo este esquema, el servicio garantiza la preservación, operación y robustecimiento de dominios estratégicos diseñados para una defensa integral del proceso. Esto incluye la implementación de un modelo de contrainteligencia para detectar insiders y canales comprometidos, así como la gestión unificada de ciberseguridad que permite anticipar ataques dirigidos. A través del monitoreo constante de la superficie de ataque y la vigilancia activa de internet y redes sociales contra la desinformación, el servicio asegura una visión completa de los recursos tecnológicos y la protección de la infraestructura de red.

Se adjunta: 2.14 HERRAMIENTAS MEDIANTE LA CREACIÓN DE DOMINIOS QUE FACILITEN EL SEGUIMIENTO DEL MARCO DE CONTROL ASOCIADO A POLÍTICAS Y NORMATIVAS APLICABLES



Actualización de hardware y software Soc.

Desde la operación SOC-CERT Se realiza de forma mensual la actualización de hardware y software de toda la infraestructura tecnológica que soporta la operación del Centro de Operaciones de Seguridad (SOC), incluyendo las plataformas de monitorización, gestión de eventos e inteligencia de seguridad, así como sus servicios asociados. Este proceso garantiza la continuidad operativa, el rendimiento óptimo de los sistemas y la mitigación de vulnerabilidades técnicas. Para ello, se cuenta con un equipo técnico especializado en infraestructura, dedicado exclusivamente a la ejecución de estas tareas de mantenimiento preventivo, correctivo y evolutivo, asegurando la disponibilidad y estabilidad de los entornos críticos para la ciberseguridad de la organización.

Se adjunta: FEBRERO



Se adjunta: MANTENIMIENTO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 3. MANTENIMIENTOS > PLANES DE MANTENIMIENTO HERRAMIENT... > 2026 > SEGUIMIENTO A MANTENIMIENTOS FEBRERO

Abre... Comentar... Copiar vínculo... Eliminar... Favorito... Agregar acceso directo... Descargar... Imprimir... Copiar en... Editar en vista de cuadrícula... Cambiar nombre... Automatizar...

Nombre	Modificado	Modificado p...	Creado	Creado por
3.11. Controlador de eventos de seguridad para la entidad y los procesos electorales -SIEM.pdf	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ
3.12. Plan de mantenimiento Aligned - informe de plataforma con la capacidad de visualizar y analizar redes...	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ
3.13. Plataforma de análisis estadístico de riesgo basada en la nube de la ENTIDAD y los procesos electorales (...)	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ
3.14. Plataforma para monitorizar la integridad de la infraestructura de seguridad electoral.pdf	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ
3.15. Sistema de Gestión Automática de Papeles para la seguridad electoral.pdf	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ
3.16. Sistema de Registro de Infraestructura Cloud.pdf	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ
3.17. Sistema de Seguridad de la Identidad.pdf	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ
3.18. Sistema que cubre el modelo de responsabilidad compartida con protecciones para nube.pdf	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ
3.19. Sistema de Gestión de Datos.pdf	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ
3.20. Sistema de Monitoreo y protección de cargas de trabajo	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ
3.21. Solución NIS para los procesos electorales.pdf	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ

Servicio Gestionado de Apoyo a la Oficina de Seguridad.

El Servicio Gestionado de Apoyo a la Oficina de Seguridad es la unidad responsable de gestionar y orquestar todos los servicios y procesos que se realizan en el Centro de Operaciones de Seguridad y están enclavados dentro de los “Servicios Gestionados de Seguridad”, los responsables estarán ubicados en la instalaciones de la Entidad en mención y tendrán un control integral del estado de las actividades que se están llevando a cabo a través de indicadores claves de rendimiento (KPIs) y cuadros de mando que permitirán la toma de decisiones a nivel ejecutivo.

También provee a la Entidad valores únicos de seguridad que representen el nivel de riesgo actual del organismo en cada una de sus partes críticas, y ofrecer una visión unificada de las amenazas y la evolución de los planes de acción implementados.

Se adjunta: 02. FEBRERO 2026

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.16 SERVICIO GESTIONADO DE APOYO A ... > 02. FEBRERO 2026

Todos los documentos + Agregar vista

Nombre	Modificado	Modificado p...	Creado	Creado por
2.0 Security Project Management Office - SPMO.pdf	21 de febrero	Venny FERNANDEZ PEREZ	21 de febrero	Venny FERNANDEZ PEREZ

Instrumento de Evaluación de Terceros:

Se ha implementado un Instrumento de Evaluación de Terceros con el objetivo de analizar y calificar los niveles de madurez, cumplimiento y riesgos asociados a los proveedores estratégicos que prestan servicios relacionados con la ciberseguridad y la infraestructura tecnológica. Esta evaluación está basada en estándares y marcos internacionales reconocidos, tales como:

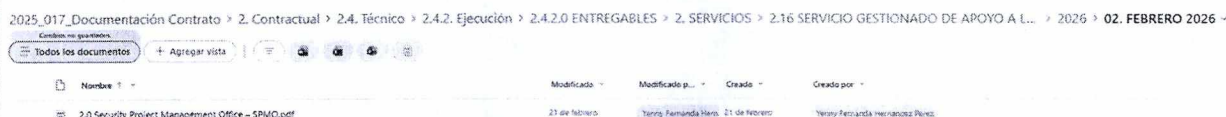
- ISO/IEC 27001: para verificar la existencia y eficacia de un Sistema de Gestión de Seguridad de la Información (SGSI);

FRR Fondo Rotatorio 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

- ISO 22301: que permite evaluar la capacidad de los proveedores para garantizar la continuidad del negocio;
- ISO 20000-1: que establece requisitos para la gestión de servicios de TI de forma eficaz y orientada al cliente;
- CMMI y SPICE/ISO 15504-12207: como referencia para evaluar la madurez de los procesos de desarrollo, mantenimiento y operación de software;
- SSAE 16 / ISAE 3402: que permiten valorar la robustez de los controles internos en organizaciones de servicios mediante informes de auditoría independientes.

Se adjunta: 02. FEBRERO 2026



Instrumento de Evaluación Controles CIS:

Se ha implementado un instrumento de evaluación de ciberseguridad fundamentado en los Controles CIS (Center for Internet Security Controls), con el propósito de medir el nivel de cumplimiento, madurez y exposición al riesgo de los entornos tecnológicos evaluados. Este marco, ampliamente reconocido a nivel internacional, proporciona un conjunto de prácticas priorizadas y accionables orientadas a proteger sistemas, redes y activos de información contra amenazas comunes.

El instrumento se basa principalmente en los CIS Controls v8, los cuales agrupan los controles en tres niveles de implementación (IG1, IG2 e IG3) según el perfil de riesgo y capacidad organizacional. La evaluación incluye controles clave como: inventario y control de activos, gestión de vulnerabilidades, protección contra malware, control de privilegios, defensa de red, monitoreo continuo, y respuesta a incidentes, entre otros.

Se adjunta: CONTROLES CIS



FRR Fondo Rotatorio 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

Evaluación de Terceros

Se ha diseñado y estructurado por cada capítulo un instrumento formal de evaluación y seguimiento de las obligaciones contractuales asociadas a los procesos electorales de la Registraduría Nacional del Estado Civil (RNEC), con el propósito de fortalecer los mecanismos de control, supervisión y aseguramiento tecnológico.

Este instrumento permite realizar una revisión detallada, sistemática y trazable de las obligaciones técnicas establecidas en los contratos, especialmente aquellas relacionadas con infraestructura tecnológica, ciberseguridad, protección de datos, continuidad del servicio, monitoreo, gestión de incidentes y cumplimiento normativo.

Se adjunta: INSTRUMENTOS

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.16 SERVICIO GESTIONADO DE APOYO A L... > **EVALUACIÓN DE TERCEROS**

Cambiar no guardado			
Todos los documentos			
+ Agregar vista			
Nombre	Modificado	Modificado por	Creado por
1. CAPÍTULO I - COMPONENTE TÉCNICO.xlsx	Hace 2 minutos	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
2. CAPÍTULO II - CANDIDATOS - COMPONENTE TÉCNICO.xlsx	Hace 2 minutos	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
3. CAPÍTULO III - COMPONENTE TÉCNICO DE JURADOS DE VOTACIÓN.xlsx	Hace 2 minutos	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
4. CAPÍTULO IV - KIT ELECTORAL COMPONENTE TÉCNICO.xlsx	Hace un minuto	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
5. CAPÍTULO IX - COMPONENTE TÉCNICO ESCRUTINIOS.xlsx	Hace un minuto	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
6. CAPÍTULO V COMPONENTE TÉCNICO.xlsx	Hace un minuto	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
7. CAPÍTULO VI - COMPONENTE TÉCNICO PARA LA AUTENTICACIÓN BIOMÉTRICA.xlsx	Hace un minuto	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
8. CAPÍTULO VII COMPONENTE TÉCNICO.xlsx	Hace un minuto	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
9. CAPÍTULO VIII - PRECONTEO Y COMUNICACIONES COMPONENTE TÉCNICO.xlsx	Hace un minuto	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
10. CAPÍTULO X - ACTA DE ESCRUTINIO DE MESA DE LOS JURADOS DE VOTACIÓN.xlsx	Hace un minuto	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
11. CAPÍTULO XI - ACTAS DE INSTALACIÓN Y REGISTRO DE VOTANTES E-11.xlsx	Hace un minuto	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
12. CAPÍTULO XII COMPONENTE TÉCNICO.xlsx	Hace un minuto	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ
13. CAPÍTULO XIII - MESA DE AYUDA COMPONENTE TÉCNICO.xlsx	Hace unos segundos	Yenny Fernanda HERNÁNDEZ PEREZ	Yenny Fernanda HERNÁNDEZ PEREZ

Instrumento de Evaluación RNEC ISO27001-2022:

Se ha desarrollado e implementado un Instrumento de Evaluación para la RNEC (Registraduría Nacional del Estado Civil) alineado con la norma ISO/IEC 27001:2022, con el objetivo de verificar el grado de cumplimiento y madurez del Sistema de Gestión de Seguridad de la Información (SGSI) dentro de los procesos y activos tecnológicos de la entidad. Esta herramienta permite identificar fortalezas, brechas y áreas críticas en la implementación de controles, facilitando la toma de decisiones informadas para la mejora continua.

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

Aprobado:
06/06/2017

El instrumento está estructurado conforme a los requisitos actualizados de la norma ISO 27001:2022, incluyendo aspectos clave como el análisis del contexto organizacional, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora. Además, evalúa de forma detallada los 93 controles del Anexo A, los cuales están agrupados en las siguientes áreas temáticas: Controles Organizacionales, Controles de Personas, Controles Físicos y Controles Tecnológicos.

Se adjunta: MSPI



Instrumento Verificación de Controles MSPI:

Se ha elaborado una Tabla de Verificación de Controles para el Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de evaluar de manera estructurada el cumplimiento de los controles exigidos por este marco normativo, el cual rige la gestión de la seguridad de la información en entidades del Estado colombiano. Este documento permite verificar el alineamiento de los procesos, activos y sistemas tecnológicos con los principios, políticas y dominios establecidos por el MSPI.

La tabla está organizada según los dominios de control definidos en el modelo, tales como: Gobierno de la Seguridad de la Información, Gestión de Riesgos, Protección de Activos de Información, Seguridad Física y Ambiental, Gestión de Incidentes de Seguridad, Continuidad del Negocio, entre otros. Cada control es evaluado con base en criterios de cumplimiento, nivel de madurez y evidencia documentada, lo que facilita la identificación de brechas y la definición de planes de acción correctivos y preventivos.

Este instrumento constituye una herramienta clave para asegurar la conformidad con el MSPI, fortalecer la postura de ciberseguridad institucional y avanzar hacia un modelo de gestión de la información basado en riesgos, trazabilidad y mejora continua.

Riesgos

Se realiza la evaluación de riesgos sobre los servicios de ciberseguridad implementados, aplicando una metodología estructurada y documentada conforme a los lineamientos de las normas ISO 31000 (Gestión del Riesgo) e ISO 27005 (Gestión de Riesgos de Seguridad de la Información), en concordancia con las directrices

FRR Fondo Rotatorio 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

emitidas por el DAFP (Departamento Administrativo de la Función Pública) en materia de administración del riesgo en entidades públicas. Este proceso permite identificar, analizar y valorar los riesgos asociados a la operación de los servicios tecnológicos, considerando amenazas, vulnerabilidades, impactos sobre la confidencialidad, integridad y disponibilidad de la información, así como riesgos operativos y reputacionales. Como resultado, se definen e implementan tratamientos de riesgo proporcionales y priorizados, orientados a fortalecer la resiliencia institucional, garantizar la continuidad del servicio y asegurar el cumplimiento del marco normativo aplicable.

Se adjunta: RIESGOS

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.16 SERVICIO GESTIONADO DE APOYO A L... > RIESGOS > 02. FEBRERO 2026

Controlar los documentos

Todos los documentos + Agregar vista

Nombre	Modificado	Modificado por	Creado	Creado por
28 Riesgos SOC-CERT 2026 (1).xlsx	21 de febrero	Nery Fernando Nieto	21 de febrero	Nery Fernando Hernandez Perez
Actividades de controles implementadas a riesgos en 1 periodo (1).xlsx	21 de febrero	Nery Fernando Nieto	21 de febrero	Nery Fernando Hernandez Perez
Riesgos materializados SOC-CERT del 15 de Enero al 14 de febrero 2026.xlsx	21 de febrero	Nery Fernando Nieto	21 de febrero	Nery Fernando Hernandez Perez

Simulación ataques cibernéticos

El servicio propuesto corresponde a una plataforma especializada de simulación avanzada de ciberataques bajo demanda, diseñada para evaluar de manera continua, realista y controlada la efectividad de las defensas de ciberseguridad de la organización.

La solución permite ejecutar escenarios personalizados a lo largo de toda la cadena de ataque, alineados con el marco MITRE ATT&CK, incorporando técnicas, tácticas y procedimientos utilizados por actores de amenaza reales (APT), incluyendo movimientos laterales, evasión de controles y explotación de vectores de red y punto final.

El servicio facilita la ejecución de pruebas en entornos seguros y aislados, utilizando imágenes controladas y artefactos de amenaza conocidos y personalizados, lo que permite medir objetivamente la capacidad de detección, respuesta y mitigación de los equipos de seguridad.

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.17 SIMULACIÓN ATAQUES CIBERNÉTICOS > 02. FEBRERO 2026

Controlar los documentos

Todos los documentos + Agregar vista

Nombre	Modificado	Modificado por	Creado	Creado por
2.17. Servicio de simulación ataques cibernéticos.pdf	Hace un minuto	Nery Fernando Nieto	Hace un minuto	Nery Fernando Hernandez Perez

FRR Fondo Rotatorio 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

Servicio de Gestión de Postura de punto de Seguridad del dato.

Este servicio está orientado a la gestión y fortalecimiento continuo de la postura de seguridad del dato en los activos de la organización, mediante un motor de Prevención de Pérdida de Datos que identifica, monitorea y bloquea en tiempo real la transferencia de información sensible. Administrado desde una plataforma centralizada de gestión, el servicio permite la aplicación y ajuste dinámico de políticas de seguridad sobre los activos de la organización, garantizando la protección de la información en sus tres estados: datos en uso, en movimiento y en reposo. Incorpora capacidades avanzadas de clasificación y detección de datos sensibles, utilizando huellas digitales tanto para información estructurada, como bases de datos, como para información no estructurada, incluyendo documentos.

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.18 GESTIÓN DE POSTURA DE SEGURIDAD ... > 02. FEBRERO 2026 ~

Todos los documentos		+ Agregar vista			
Nombre	Modificado	Modificado p...	Creado	Creado por	
2.18. Gestión de postura de seguridad del dato - Informe Operativo.docx.pdf	El jueves a las 21:04	Nery Fernando Hain	El jueves a las 21:08	Nery Fernando Hernández Pérez	
2.18. Gestión de postura de seguridad del dato.pdf	El jueves a las 21:07	Nery Fernando Hain	El jueves a las 21:07	Nery Fernando Hernández Pérez	

Servicio de protección y prevención de amenazas contra la información en el punto final.

Este servicio está orientado a la protección y prevención de amenazas contra la información mediante la gestión continua de la postura de seguridad de los datos, permitiendo el descubrimiento, clasificación y mapeo de información sensible en los activos de la organización. A través de capacidades de la solución, el servicio identifica datos estructurados y no estructurados en la entidad, proporcionando visibilidad sobre qué información existe, dónde se encuentra y qué nivel de sensibilidad y contexto empresarial posee. Con base en este análisis, evalúa y prioriza los riesgos asociados al manejo de la información, tales como accesos con privilegios excesivos, ubicaciones inadecuadas o configuraciones inseguras, permitiendo su corrección o remediación. Adicionalmente, el servicio realiza monitoreo continuo para mantener actualizada la postura de seguridad del dato, fortalecer los controles de protección en el punto final y apoyar de forma efectiva la operación de las soluciones de prevención de pérdida de datos, reduciendo el riesgo de exposición o uso indebido de la información.

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.19 PROTECCIÓN Y PREVENCIÓN DE AME... > 02. FEBRERO 2026 ~

Todos los documentos		+ Agregar vista			
Nombre	Modificado	Modificado p...	Creado	Creado por	
2.19. Protección y prevención de amenazas contra la información en el punto final - Informe Operativo.pdf	El jueves a las 21:41	Nery Fernando Hain	El jueves a las 21:40	Nery Fernando Hernández Pérez	
2.19. Protección y prevención de amenazas contra la información en el punto final.pdf	El jueves a las 21:40	Nery Fernando Hain	El jueves a las 21:40	Nery Fernando Hernández Pérez	

FRR Fondo Rotatorio 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

Servicio de protección y prevención de amenazas contra la información en la nube

Este servicio proporciona control y protección integral sobre el uso de servicios en la nube, monitoreando y aplicando políticas de seguridad en tiempo real sobre entornos de productividad como Office 365. A través de capacidades avanzadas de CASB, el servicio previene la carga, descarga y distribución inapropiada de información sensible o clasificada, asegurando el cumplimiento de las políticas corporativas y regulatorias. Permite el descubrimiento automático de aplicaciones en la nube utilizadas por los funcionarios, incluyendo aquellas no autorizadas (Shadow IT), y analiza continuamente las actividades para detectar y bloquear comportamientos de riesgo. El servicio aplica principios de Zero Trust basados en el contexto del usuario y del dispositivo, controla sesiones para su interrupción inmediata ante eventos sospechosos, detecta accesos anómalos como inicios de sesión en horarios inusuales o desde ubicaciones geográficas no habituales, se integra con el directorio corporativo para una correcta identificación y control de privilegios, cifra la información en tránsito hacia la nube y genera reportes ejecutivos y operativos listos para auditoría. Todo ello brinda visibilidad completa, control preciso y cumplimiento automático de las normas de seguridad de la información en entornos cloud.

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.20 PROTECCIÓN Y PREVENCIÓN DE AME... > 02. FEBRERO 2026 <				
Todos los documentos + Agregar vista				
Nombre				
2.20 Protección y prevención de amenazas contra la información en la nube informe operativo.pdf	Última a las 22:07	Ver	Modificar	Eliminar
2.20 Protección y prevención de amenazas contra la información en la nube.pdf	Última a las 22:07	Ver	Modificar	Eliminar

Servicio de protección y monitoreo de información en Estático, Tránsito y Consumo

Este servicio proporciona una capa de protección persistente de la información mediante mecanismos de cifrado y gestión centralizada de permisos, garantizando que los datos permanezcan protegidos incluso cuando salen del perímetro y del control directo de la red corporativa. A través de la implementación y gestión de la solución, el servicio permite controlar el acceso y uso de la información de forma continua, asegurando su protección en los estados de información en reposo (estático), en tránsito y en consumo.

Se adjunta: FEBRERO

2025_017_Documentación Contrato > 2. Contractual > 2.4. Técnico > 2.4.2. Ejecución > 2.4.2.0 ENTREGABLES > 2. SERVICIOS > 2.21 SERVICIO DE PROTECCIÓN Y MONITO... > 02. FEBRERO 2026 <				
Todos los documentos + Agregar vista				
Nombre				
2.21 Protección y monitoreo de información en estático, tránsito y consumo - Informe Operativo.pdf	Última a las 17:48	Ver	Modificar	Eliminar
2.21 Protección y monitoreo de información en estático, tránsito y consumo.pdf	Última a las 17:48	Ver	Modificar	Eliminar

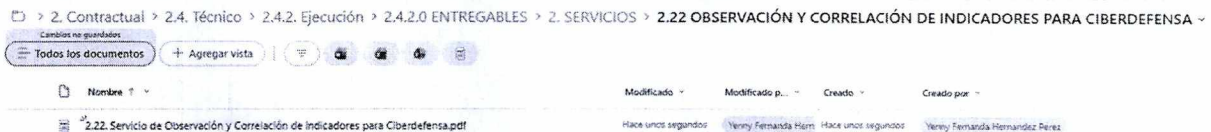
PROCESO	GESTIÓN CONTRACTUAL	CÓDIGO	GCFT08
FORMATO	INFORME DE SEGUIMIENTO DE SUPERVISIÓN Y/O INTERVENTORIA	VERSIÓN	0

Aprobado:
06/06/2017

A. Servicio de Observación y Correlación de Indicadores para Ciberdefensa

El servicio proporciona capacidades avanzadas para la observación, categorización, correlación y enriquecimiento automático de la información asociada a indicadores de compromiso (IoC), permitiendo una visión integral y contextualizada de las amenazas que afectan a la organización. El servicio se integra de forma nativa con tecnologías de seguridad como firewalls, SIEM, SOAR, proxies y EDR, utilizando protocolos estandarizados como STIX y TAXII, lo que mejora significativamente el análisis, la detección y la respuesta. Incorpora automatización de acciones de respuesta sobre distintos controles de seguridad y plataformas de gestión, así como mecanismos de intercambio de inteligencia tanto entre áreas internas como con organizaciones externas. Proporciona inteligencia consolidada sobre adversarios, habilita una plataforma completa de búsqueda para investigaciones forenses y suministra datos de alta calidad sobre amenazas relevantes, ajustadas al sector, geografía y contexto de riesgo del cliente.

Se adjunta: FEBRERO



Se adjuntan: INFORME DE ACTIVIDADES Adición Pago NO. 2

Se adjunta los informes de las actividades desarrolladas Adición Pago NO. 2 entregado por el contratista que cuenta con las especificaciones técnicas:

- Estado actual del servicio.
- Soluciones tecnológicas desplegadas.

Este informe y sus anexos son considerados de carácter reservado garantizando la Defensa y Seguridad Nacional.

De acuerdo con lo anterior, la supervisión del contrato confirma que el contratista cumple con los requerimientos establecidos en el contrato 017 de 2025.

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.

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

Aprobado:
06/06/2017

BALANCE FINANCIERO:

CONTRATO 017 DE 2025 - UNE	
VALOR DEL CONTRATO	\$ 29.309.990.000
PAGO 1 - Equivalente al 25% del valor del contrato, correspondiente al avance del cronograma de las actividades (Corporate security intelligence, vigilancia digital & cyber threat intelligence, auditorías técnicas de seguridad, monitorización de eventos de seguridad, respuesta a incidentes, gestión de crisis de seguridad, Threat Hunting, alerta temprana, alertas preventivas, servicios para la atención de eventos de y para la infraestructura tecnológica basados en mejores prácticas ITIL).	\$ 7.303.539.000
PAGO 2 – Equivalente al 20% del valor del contrato, correspondiente al avance del cronograma de las actividades (Corporate security intelligence, vigilancia digital & cyber threat intelligence, auditorías técnicas de seguridad, monitorización de eventos de seguridad, respuesta a incidentes, gestión de crisis de seguridad, Threat Hunting, alerta temprana, alertas preventivas, servicios para la atención de eventos de y para la infraestructura tecnológica basados en mejores prácticas ITIL, gestión de la respuesta ante la identificación y remediación de vulnerabilidades en plataforma tecnológica, generar un conjunto de herramientas mediante la creación de dominios que faciliten el seguimiento del marco de control asociado a políticas y normativas aplicables, actualización de hardware y software SOC, y Servicio Gestionado de Apoyo a la Oficina de Seguridad) descritas en el cuadro anterior, previa certificación e informe de actividades entregadas suscrito por parte del supervisor del contrato.	\$ 5.768.691.250
PAGO 3 – Equivalente al 24% del valor del contrato, correspondiente al avance del cronograma de las actividades (Corporate security intelligence, vigilancia digital & cyber threat intelligence, auditorías técnicas de seguridad, monitorización de eventos de seguridad, respuesta a incidentes, gestión de crisis de seguridad, Threat Hunting, alerta temprana, alertas preventivas, servicios para la atención de eventos de y para la infraestructura tecnológica basados en mejores prácticas ITIL, gestión de la respuesta ante la identificación y remediación de vulnerabilidades en plataforma tecnológica, previa certificación e	\$ 7.175.505.250

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

Aprobado:
06/06/2017

informe de actividades entregadas suscrito por parte del supervisor del contrato.	
PAGO 4 – Equivalente al 17% del valor del contrato, correspondiente al avance del cronograma de las actividades (Corporate security intelligence, vigilancia digital & cyber threat intelligence, auditorías técnicas de seguridad, monitorización de eventos de seguridad, respuesta a incidentes, gestión de crisis de seguridad, Threat Hunting, alerta temprana, alertas preventivas, servicios para la atención de eventos de y para la infraestructura tecnológica basados en mejores prácticas ITIL, gestión de la respuesta ante la identificación y remediación de vulnerabilidades en plataforma tecnológica, previa certificación e informe de actividades entregadas suscrito por parte del supervisor del contrato.	\$ 4.915.897.250
PAGO 5 – Equivalente al 14% del valor del contrato, correspondiente al avance del cronograma de las actividades (Corporate security intelligence, vigilancia digital & cyber threat intelligence, auditorías técnicas de seguridad, monitorización de eventos de seguridad, respuesta a incidentes, gestión de crisis de seguridad, Threat Hunting, alerta temprana, alertas preventivas, servicios para la atención de eventos de y para la infraestructura tecnológica basados en mejores prácticas ITIL, gestión de la respuesta ante la identificación y remediación de vulnerabilidades en plataforma tecnológica, previa certificación e informe de actividades entregadas suscrito por parte del supervisor del contrato.	\$ 4.146.357.250
SALDO	\$ 0

FRR Fondo Rotatorio 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

ADICIÓN Y OTROSÍ No. 01 Y PRÓRROGA No. 02 AL CONTRATO 017 DE 2025	
VALOR DE LA ADICIÓN	\$ 13.102.945.424
Pago 1. Avance del cronograma de las actividades (Corporate security intelligence, vigilancia digital & cyber threat intelligence, auditorías técnicas de seguridad, monitorización de tos de seguridad, respuesta a incidentes, gestión de crisis de seguridad, Threat Hunting, alerta temprana, alertas preventivas, servicios para la atención de eventos de y para la infraestructura tecnológica basados en mejores prácticas ITIL.)	\$ 1.100.247.324
Pago 2. - Servicio de Gestión de Postura de Seguridad del Dpto. - Servicio de protección y prevención de amenazas contra la información en el punto final. - Servicio de protección y prevención de amenazas contra la información en la nube. - Servicio de protección y monitoreo de información en estático, tránsito y consumo. - Servicio de observación y correlación de indicadores para Ciberdefensa.	\$ 3.000.674.525
SALDO	\$ 9.002.023.575

De acuerdo con lo anterior, la supervisión del contrato confirma que el contratista cumple con los requerimientos establecidos en el Contrato 017 de 2025 y su Adición y Otrosí No. 1 y Prorroga No. 2.

En constancia de lo anterior, se firma el presenta informe, a los dos (2) días del mes de marzo de 2026.

SUPERVISOR


HOSLANDER ADLAI SÁENZ BARRERA
Gerente de Informática

Proyectó: Andrés Acosta Blanquiceth
Revisó: Eduardo Emilio Calderón Narvaez