ORDEN DE SERVICIO No. 1 AL CONTRATO MARCO No. 202500142_1

CONTRATO No:	**202500142_1**
CONTRATISTA:	**NSIT**
NIT:	**900.449.084-1**
OBJETO DEL CONTRATO MARCO:	Aunar esfuerzos de equipo para la ejecución de proyectos relacionados con servicios de TI, SOLUCIONES INTEGRALES DE CIBERSEGURIDAD Y SEGURIDAD DIGITAL donde se puedan sincronizar herramientas tecnológicas, capacidad instalada, y la infraestructura física existente.
PLAZO DEL CONTRATO MARCO:	El plazo es de doce (12) meses, contados desde la suscripción del contrato marco de alianza estratégica.
FECHA DE INICIO CONTRATO MARCO:	11 de Agosto de 2025
VALOR CONTRATO MARCO:	**Cuantía Indeterminada**
OBJETO DE LA ORDEN DE SERVICIO 1:	Prestación de servicios necesarios para el fortalecimiento de la seguridad informática frente a ciberamenazas
PLAZO ORDEN DE SERVICIOS No. 1:	Hasta el 31 de diciembre de 2025
VALOR ORDEN DE SERVICIOS No.1:	**SETECIENTOS CINCUENTA Y SIETE MILLONES DOSCIENTOS OCHENTA Y OCHO MIL SEISCIENTOS NOVENTA Y SIETE PESOS M/L ($757.288.697)** impuestos incluidos

La presente constituye la Orden de Servicio N° 1 al Contrato Marco 202500142_1 suscrito entre la Empresa para la Seguridad y Soluciones Urbanas ESU y NSIT SAS, cuyo objeto es “Prestación de servicios necesarios para el fortalecimiento de la seguridad informática frente a ciberamenazas” previas las siguientes:

CONSIDERACIONES:

ALCANCE DE LA ORDEN Y DESCRIPCIÓN DEL SERVICIO: En desarrollo del Acuerdo Marco de la referencia, el alcance del objeto será la satisfacción de las necesidades que requieran nuestros clientes en materia de servicios de soluciones de tecnologías de información y de las comunicaciones identificadas como herramientas que pueden aportar al control para mitigar riesgos de seguridad informática frente a ciberamenazas y servicios especializados de seguridad informática que podrían aportar a mejorar la postura de Seguridad Informática frente a Ciberamenazas.

ESPECIFICACIONES TÉCNICAS ASOCIADAS A SERVICIOS DE SEGURIDAD INFORMÁTICA ESPECIALIZADOS

1. SERVICIO DE MONITOREO CONTINUO DE EVENTOS E INCIDENTES DE SEGURIDAD INFORMÁTICA SOBRE LA INFRAESTRUCTURA TECNOLÓGICA DEL DISTRITO DE MEDELLÍN PRIORIZADA FRENTE A CIBERAMENAZAS

Objetivo:

Generar las notificaciones para la atención oportuna relacionadas con eventos y/o alertas debidamente analizadas, valoradas y clasificadas, a través del monitoreo continuo apoyado en herramientas de visualización de eventos y alertas, herramientas de correlación de eventos y herramientas para la respuesta automatizada a partir de las fuentes de información de logs de seguridad informática internos suministrados y de eventos de seguridad informática externos generados, así como de la revisión de plataformas de gestión de eventos de seguridad informática institucionales, que aporten a la detección y gestión oportuna de eventos, alertas o incidentes detectados frente a ciberamenazas.

Características:

- ✓ Ejecutar las actividades de apoyo a la implementación de una solución de recolección de fuentes de información (Agentes y Colector Centralizado) on premise, para la consolidación de la información de eventos de seguridad informática priorizados para la transferencia hacia la solución SIEM incluida en el servicio.
- ✓ Ejecución de las actividades de Integración de fuentes de información generada a través de las soluciones SIEM definidas, hacia la plataforma SOAR incluida en el servicio.
- ✓ Ejecución de las actividades requeridas para lograr la ingesta de fuentes de información sobre eventos de seguridad de activos informáticos institucionales (Hasta 20 fuentes de información) e integración a la solución SIEM incluida en el servicio.
- ✓ Ejecución de las actividades requeridas para el desarrollo continuo de casos de uso de correlación de eventos de seguridad informática basados en única fuente, orientados a la gestión de eventos y alertas desde la plataforma SIEM incluida en el servicio, por necesidades identificadas por el proveedor o por el cliente.
- ✓ Ejecución de las actividades requeridas para el desarrollo continuo de casos de uso de correlación de eventos de seguridad informática basados en múltiples fuentes para la correlación de eventos, orientados a la gestión de eventos y alertas desde la plataforma SIEM incluida en el servicio, por necesidades identificadas por el proveedor o por el cliente.

- ✓ Ejecución de las actividades requeridas para el desarrollo continuo de casos de uso de automatización de la respuesta de seguridad informática frente a ciberamenazas, orientados a la integración de acciones con herramientas o soluciones institucionales para la gestión de eventos, alertas o incidentes de seguridad informática identificados, por necesidades identificadas por el proveedor o por el cliente.
- ✓ Ejecución de las actividades de Monitoreo 7 x 24 de eventos, alertas o incidentes sobre la plataforma SIEM incluida en el servicio a partir de las fuentes de información integradas.
- ✓ Ejecución de las actividades de Monitoreo 7 x 24 de eventos, alertas o incidentes sobre la plataforma SPLUNK dispuesta por el Distrito de Medellín, a partir de las fuentes de información integradas a la misma.
- ✓ Ejecución de las actividades de Monitoreo 7 x 24 de eventos o alertas de seguridad informática detectados sobre la plataforma FORTIRECON dispuesta por el Distrito de Medellín, a partir de eventos relacionados con afectaciones a la superficie de ataque institucional, afectación a la imagen institucional, o a la suplantación de las plataformas institucionales y a la filtración de datos en la Dark web o Deep web.
- ✓ Ejecución de las actividades de Monitoreo 7 x 24 de eventos y/o alertas generadas por las plataformas de seguridad informática institucionales de la Entidad priorizadas, a partir de eventos relacionados de malware, de comportamiento o de accesos no autorizados, identificación de inteligencia de amenazas y vulnerabilidades identificadas a través de la solución.
- ✓ Ejecución de las actividades de análisis, clasificación y valoración de eventos y/o alertas críticos y generación de reportes (Hallazgo, análisis y recomendaciones) para la toma de decisiones institucional.
- ✓ Ejecución de las actividades requeridas para el mantenimiento actualizado de una base de datos de eventos y/o alertas conocidas, que permita reconocer y establecer un tratamiento estándar oportuno y adecuado.
- ✓ Ejecución de las actividades requeridas para la generación de requerimientos hacia la Entidad, para la atención de eventos y/o alertas identificadas, describiendo las acciones de mejora requeridas.
- ✓ Ejecución de las actividades requeridas para socializar semanalmente el estado de la atención de eventos, alertas o incidentes detectados, así como de las acciones de mejora propuesta, en articulación con el personal de seguridad informática del distrito de Medellín

Metodología:

- ✓ Planeación del Servicio: A través de la planeación del servicio se definen las condiciones de operación, los flujos actuación, de temporización, de articulación

y de generación de informes, de acuerdo con lo definido en las especificaciones técnicas del servicio.

- ✓ Ejecución del Servicio: Se ejecutan las acciones que se requieran para lograr una estabilización que permita mejorar la ejecución de las actividades incluidas en el servicio, de acuerdo con lo definido en las especificaciones técnicas. Adicionalmente, se ejecutan las actividades misionales del servicio, de acuerdo con lo planeado y en cumplimiento de las especificaciones técnicas definidas.
- ✓ Seguimiento a la prestación del Servicio: Se ejecutan acciones de generación, presentación, revisión y ajustes de informes definidos, así como de reuniones de seguimiento a la prestación, documentación y cumplimiento del servicio, así como de la definición de acciones de mejora continua del servicio cuando sea necesario, de acuerdo con lo establecido en las especificaciones técnicas del servicio.
- ✓ Finalización del Servicio: Se verifica el cumplimiento de los entregables y de las condiciones de prestación del servicio definidas en el marco de las especificaciones técnicas del servicio.

Capacidades Disponibles del Servicio

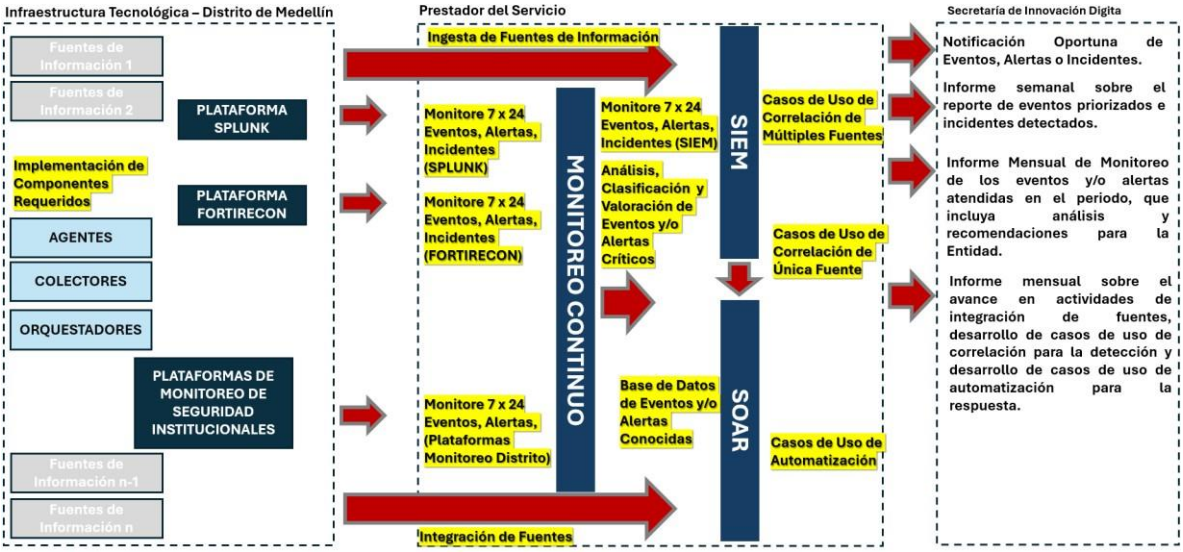
- ➢ **Soluciones Tecnológicas Incluidas en el Servicio**
  - ✓ Solución SIEM
  - ✓ Software de Agentes y Colectores para SIEM
  - ✓ Solución SOAR
  - ✓ Software de Agentes y Configuraciones para SOAR
- ➢ **Roles y Personal Requerido**
  - **Personal en Instalaciones del Proveedor**
    - ✓ Lider de Soc
    - ✓ Analista de SOC Nivel 2
    - ✓ Analista de SOC Nivel 1
  - **Personal en Instalaciones del Cliente**
    - ✓ Enlace de Operación con el SOC
    - ✓ Analista de SOC Nivel 2

Modelo de Prestación del Servicio:

En atención a la planeación y preparación del servicio se definen las actividades que se deben colocar en marcha para la prestación del servicio solicitado, teniendo en cuenta las actividades para la integración de fuentes de información a la solución SIEM incluida en el servicio, el acceso a las plataformas o herramientas de monitoreo institucionales que serán incluidas como parte de la prestación del servicio de monitoreo continuo contratado.

La ejecución del servicio debe garantizar los servicios de monitoreo continuo 7 x 24 a partir de las plataformas priorizadas por el Distrito de Medellín y garantizar la

notificación oportuna de eventos y/o alertas o el reporte de incidentes detectados durante la prestación de este servicio. Así mismo, el prestador de servicio realizará las actividades para el análisis, clasificación y valoración de los eventos y/o alertas críticas y mantendrá actualiza una base de datos de eventos y/o alertas conocidas, que da cuentas de la actuación del prestador del servicio ante su detección y aporta a la Entidad un conjunto de pasos definidos para la atención de estos. Por otro lado, el prestador del servicio debe avanzar de manera permanente en la definición y desarrollo continuo de casos de uso de correlación de eventos a partir de una única fuente o de múltiples fuentes, así como para la definición y desarrollo continuo de casos de uso para la automatización de la respuesta apoyado en las capacidades de la herramienta SOAR.



La entidad realizará actividades de seguimiento a partir de las salidas definidas como parte de la prestación del servicio, buscando siempre el cumplimiento de las actividades encomendadas y la mejora permanente de la prestación de los servicios contratados.

Entregables:

- ✓ Plan de Prestación del Servicio, que aborde las actividades de monitoreo, notificación de eventos e incidentes, de integración de fuentes, de consolidación de casos de uso, así como de instalación de agentes o componentes que puedan ser requeridos en la prestación del servicio.
- ✓ Informe semanal sobre el reporte de eventos priorizados e incidentes detectados.
- ✓ Informe Mensual de Monitoreo de los eventos y/o alertas atendidas en el periodo, que incluya análisis y recomendaciones para la Entidad.
- ✓ Informe mensual sobre el avance en actividades de integración de fuentes, desarrollo de casos de uso de correlación para la detección y desarrollo de casos de uso de automatización para la respuesta.

2. SERVICIO DE APOYO A LA GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA FRENTE A CIBERAMENAZAS

Objetivo:

Ejecutar de manera articulada con la Entidad, las actividades de preparación y tratamiento de incidentes de seguridad informática frente a ciberamenazas; a través de la identificación, seguimiento y apoyo a la generación de capacidades, habilidades y competencias para el tratamiento de incidentes de seguridad informática frente a ciberamenazas, así como a través del diseño e implementación continua de casos de uso que permiten adoptar procesos automatizados de respuesta; que aporten al fortalecimiento de las capacidades institucionales para la detección y respuesta oportuna ante la materialización de incidentes de seguridad informática frente a ciberamenazas.

Características:

- ✓ Apoyar a la Entidad en la identificación de Capacidades, Competencias y Habilidades para la Detección, Respuesta y Recuperación ante Incidentes.
- ✓ Apoyar a la Entidad a través del acompañamiento a los corresponsables de la plataforma informática, para el diseño de planes de fortalecimiento de capacidades, competencias y habilidades para la detección, respuesta y recuperación ante incidentes, así como al seguimiento y la evaluación de estos.
- ✓ Apoyar a la Entidad en la identificación y diseño de casos de uso para aplicar soluciones automatizadas tipo SOAR para mejorar la oportunidad en la respuesta a incidentes de seguridad informática frente a ciberamenazas.
- ✓ Apoyar a la Entidad en la implementación de casos de uso automatizadas de tipo SOAR, para la puesta en producción, operación, seguimiento y mejora; para mejorar la oportunidad en la respuesta a incidentes de seguridad informática frente a ciberamenazas.
- ✓ Apoyar a la Entidad en la ejecución de actividades de análisis, valoración, clasificación y priorización para la atención de incidentes de seguridad informática frente a ciberamenazas
- ✓ Apoyar a la Entidad en la ejecución de actividades que se derivan de la detección de un incidente de seguridad informática, orientadas al diagnóstico, investigación, mitigación, contención, erradicación, recuperación y aprendizaje durante el tratamiento de incidente.
- ✓ Apoyar la construcción de los planes de gestión de incidentes basados en casos de uso y su actualización.

Metodología:

- ✓ Planeación del Servicio: Se define el plan de trabajo respecto de las necesidades institucionales y la misionalidad del servicio, de acuerdo con las especificaciones técnicas definidas.

- ✓ Ejecución del Servicio: Se ejecutan las actividades definidas en el plan de trabajo concertado, de acuerdo con las especificaciones técnicas definidas.
- ✓ Seguimiento a la prestación del Servicio: Se verifica el avance en la ejecución de las actividades y se generan y presentan informes sobre las actividades ejecutadas, de acuerdo con las especificaciones técnicas definidas.
- ✓ Finalización del Servicio: Se verifica el cumplimiento de los entregables y de las actividades definidas en el plan de trabajo concertado, de acuerdo con las especificaciones técnicas definidas.

Capacidades Disponibles del Servicio:

- ➢ **Soluciones Tecnológicas Incluidas en el Servicio**

Solución SOAR

Software de Agentes y Configuraciones para SOAR

- ➢ **Personal**
  - **Personal en Instalaciones del Proveedor**
    - ✓ Analista de SOC Nivel 2
  - **Personal en Instalaciones del Cliente**
    - ✓ Analista de SOC Nivel 2

Modelo de Prestación del Servicio:

En atención a la planeación del servicio se definen las actividades requeridas para la prestación del servicio, las cuales tienen tres enfoques de trabajo articulados, a saber: el fortalecimiento de un modelo Institucional de Capacidades, Competencias y Habilidades para la Detección, Respuesta y Recuperación ante Incidentes; el fortalecimiento del modelo de Atención de Incidentes frente a Cibermanenazas y el modelo de diseño e implementación de Casos de Uso de Automatización.

La ejecución del servicio debe garantizar que se desarrollen las actividades planeadas, orientadas a apoyar la identificación de Capacidades, Habilidades y Competencias -C.H.C.-, y el diseño de planes para el fortalecimiento de dichas capacidades; así como las actividades requeridas a partir de la detección de un incidente, o las que se requieran en el marco del tratamiento de un incidente materializado, y el apoyo a la construcción de planes de gestión de incidentes basados en casos de uso definidos. Así mismo, la ejecución de las actividades requeridas para el diseño de casos de automatización y el apoyo a la implementación a partir de las necesidades priorizadas por el Distrito de Medellín.

La entidad realizará actividades de seguimiento a partir de los informes mensuales de avance y el reporte de los incidentes frente a ciberamenazas tratados durante el periodo, buscando siempre el cumplimiento de las actividades encomendadas de acuerdo con las especificaciones técnicas definidas.

Entregables:

- ✓ Plan de Prestación del Servicio, que aborde las actividades concertadas con la Entidad, de acuerdo con la finalidad del servicio.
- ✓ Informe mensual sobre el avance en el plan de trabajo concertado, de acuerdo con las especificaciones técnicas definidas.
- ✓ Reportes de incidentes tratados de acuerdo con los requisitos concertados y con las especificaciones técnicas definidas.

3. SERVICIO DE CACERÍA DE AMENAZAS

Objetivo:

Ejecutar actividades de cacería de amenazas basadas en análisis de información generada a partir de alertas, eventos, comportamientos, correlación, técnicas de exposición de señuelos, entre otras técnicas requeridas, a través de solicitudes de investigación apoyadas en el uso de tecnologías disponibles y personal especializado, orientadas a proponer acciones de mejora para mitigar riesgos frente a cibermamenazas. **Características:**

- ✓ Ejecución de actividades de cacería de amenazas basados en **solicitudes de investigación** priorizadas a partir de la información interna o externa sobre eventos, alertas o incidentes de seguridad informática frente a ciberamenaza detectados sobre la infraestructura o a través de ejercicios concertado para la exposición de señuelos digitales en segmentos de red interna o expuestos hacia internet; orientados a fortalecer las capacidades de detección y respuesta en el tratamiento de incidentes de seguridad informática frente a ciberamenazas.

- ✓ Ejecución de las actividades de administración y operación de la herramienta **FortiDeceptor**, en relación con la instalación, configuración, mantenimiento, actualización, generación de señuelos, transporte de estos y despliegue en máquinas virtuales, entre otros.
- ✓ Ejecución de las actividades de administración y operación de la herramienta **FortiRecon**, en relación con la configuración, mantenimiento, actualización, registro de activos, marcas, dominios, entre otros.

Metodología:

- ✓ Planeación del Servicio: Se definen de manera concertada y priorizada solicitudes de investigación, a partir de las cuales se define un plan de trabajo de cacería de amenazas, respecto de la misionalidad del servicio y de las especificaciones técnicas definidas. Así mismo, se planifican las actividades para la administración y operación de las plataformas FortiDeceptor y FortiRecon incluidas como parte de la prestación del servicio.
- ✓ Ejecución del Servicio: Desarrollar las actividades de cacería de amenazas propuestas en el plan de trabajo a partir de las solicitudes de investigación priorizadas mensualmente, en atención a las especificaciones técnicas definidas. De igual manera se ejecutan las actividades orientadas a la administración y operación de las plataformas FortiDeceptor y FortiRecon, de acuerdo con la planeación concertada y las especificaciones técnicas definidas.
- ✓ Seguimiento a la prestación del Servicio: Se verifica el avance en la ejecución de las actividades y se generan y presentan informes una vez se ha concluido la solicitud de investigación priorizada, en atención a las especificaciones técnicas definidas. De igual manera, se verifican los informes mensuales correspondientes a la ejecución de las actividades de administración y operación de las plataformas FortiDeceptor y FortiRecon.
- ✓ Finalización del Servicio: Se verifica el cumplimiento de los entregables y de las actividades definidas en cada plan de trabajo generado a partir de las solicitudes de investigación priorizadas y de acuerdo con las especificaciones técnicas definidas. Así mismo, se verifica el cumplimiento de la ejecución de las actividades correspondientes a la administración y operación de las plataformas FortiDeceptor y FortiRecon.

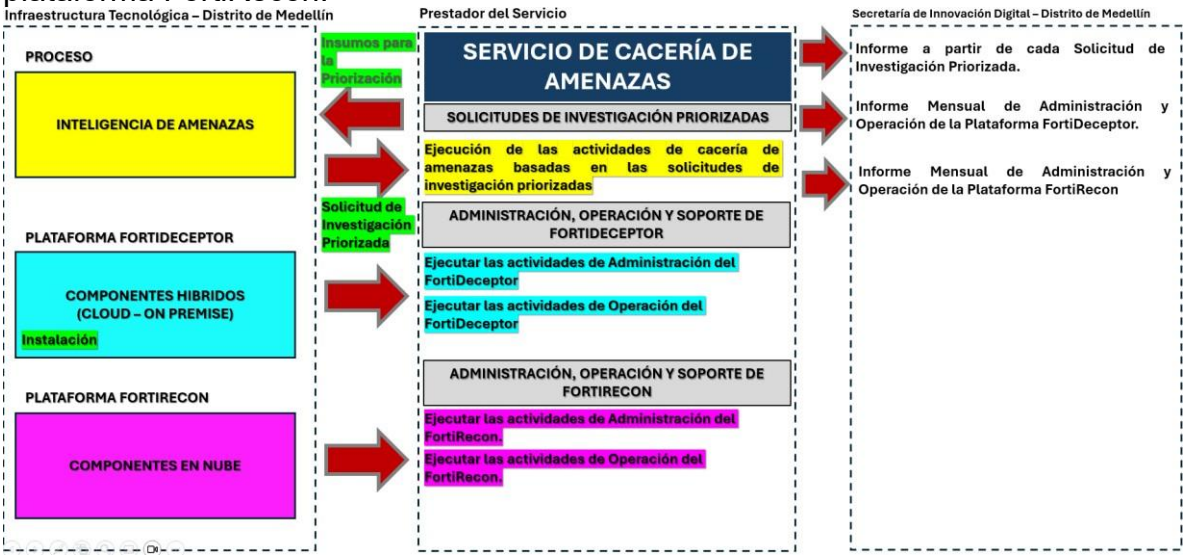
Capacidades Disponibles del Servicio:

- ➢ **Soluciones Tecnológicas**
  - ✓ Fortideceptor (Licenciadas por la Entidad)
  - ✓ Fortirecon (Licenciadas por la Entidad)

- **Personal**
  - ✓ **Personal en Instalaciones del Proveedor**
    - ✓ Especialistas en Cacería de Amenazas

Modelo de Prestación del Servicio:

En atención a la planeación del servicio se definen las actividades requeridas para la prestación del servicio, las cuales tienen tres enfoques de trabajo articulados, a saber: La ejecución de actividades de cacería de amenazas basadas en solicitudes de Investigación Priorizadas por el Distrito de Medellín; la administración y operación de la plataforma FortiDeceptor y la administración y operación de la plataforma FortiRecon.



La ejecución del servicio debe garantizar que se desarrollen las actividades planeadas, orientadas a ejecutar las actividades de cacería de amenazas a partir de las solicitudes de investigación priorizadas por el Distrito de Medellín. De la misma manera, conforme a las especificaciones técnicas definidas y a la concertación entre las partes en la etapa de planeación para la prestación del servicio, se deberán ejecutar por parte del prestador del servicio las actividades de administración y operación de las plataformas FortiDeceptor y FortiRecon, como generadoras de información de valor para la priorización de las actividades de cacería y para la ejecución de actividades de análisis y generación de informes frente a ciberamenazas.

La entidad realizará actividades de seguimiento a partir de los informes de cada solicitud de investigación priorizada, así como, los informes mensuales sobre las actividades de administración y operación de las plataformas FortiDeceptor y FortiRecon durante el periodo, buscando siempre el cumplimiento de las actividades encomendadas de acuerdo con las especificaciones técnicas definidas.

Entregables:

- ✓ Plan de Prestación del Servicio, que aborde las actividades de investigación a través de técnicas de cacería de amenazas, así como las actividades de administración y operación de FortiDeceptor y de FortiRecon, como herramientas de apoyo a la ejecución de las actividades.
- ✓ Informe a partir de cada solicitud de investigación priorizada.
- ✓ Informe mensual de administración y operación de la plataforma FortiDeceptor.
- ✓ Informe mensual de administración y operación de la plataforma FortiRecon.

4. SERVICIO DE ADMINISTRACIÓN Y OPERACIÓN DE LA PLATAFORMA DE GESTIÓN DE VULNERABILIDADES

Objetivo

Ejecutar las actividades de administración y operación de la plataforma de gestión de vulnerabilidades institucional, a través de la gestión de usuarios, módulos, configuraciones, backups, actualizaciones, entre otras responsabilidades propias de la administración; así como a través de la identificación, análisis, clasificación, evaluación, priorización y generación de informes con recomendaciones para la remediación de vulnerabilidades técnicas sobre activos informáticos de la infraestructura tecnológica institucional, así como sobre los sitios y aplicaciones web institucionales, a través de metodologías y herramientas tecnológicas de identificación de vulnerabilidades dispuestas por la Entidad, con el fin de aportar a la debida gestión de vulnerabilidades y de esta manera mitigar los riesgos a los que se expone la infraestructura tecnológica institucional.

Características:

- ✓ Ejecutar las actividades de identificación y análisis de vulnerabilidades técnicas en activos informáticos de la infraestructura tecnológica de la entidad y recomendar las remediaciones requeridas, de acuerdo con las capacidades tecnológicas y de licenciamiento disponibles; en atención a la programación definida o por demanda a través de requerimientos, de acuerdo con las especificaciones técnicas definidas.
- ✓ Ejecutar las actividades de identificación y análisis de vulnerabilidades técnicas en sitios y aplicaciones web institucionales y recomendar las remediaciones requeridas, de acuerdo con las capacidades tecnológicas y de licenciamiento disponibles; en atención a la programación definida o por demanda a través de requerimientos, de acuerdo con las especificaciones técnicas definidas.
- ✓ Ejecución de las actividades de administración y operación de la herramienta Tenable One, en relación con la configuración, mantenimiento, actualización, entre otras actividades requeridas para su disponibilidad y adecuado funcionamiento.

- ✓ Ejecutar las actividades de operación relacionadas con el descubrimiento y gestión de activos en tiempo real, el escaneo continuo de vulnerabilidades en sistemas operativos, aplicaciones, bases de datos y servicios, el escaneo y análisis de seguridad de aplicaciones web (WAS), la priorización de vulnerabilidades basada en riesgo, contexto y amenazas activas (Threat Intelligence), la generación de informes ejecutivos, técnicos y de cumplimiento, así como la integración con flujos de trabajo de remediación y automatización de respuestas, entre otras.
- ✓ Ejecutar las actividades de diseño de paneles de control interactivos y tableros personalizables, así como de reportes por actividades de escaneo realizadas, o por requerimientos del cliente.
- ✓ Ejecutar las actividades de apoyo a la implementación de agentes o soluciones en la infraestructura on premise de la entidad, que sean requeridas para la correcta ejecución de las actividades de identificación y gestión de vulnerabilidades.

Metodología:

- ✓ Planeación del Servicio: Se define el plan de trabajo para la priorización de las actividades de identificación de activos informáticos, la ejecución de las actividades de escaneo programadas o por demanda, la articulación de las actividades con el personal del área de tecnología de la Entidad, así como de las actividades relacionadas con la administración y operación de la plataforma Tenable One, entre otras requeridas para la prestación del servicio, de acuerdo con las especificaciones técnicas definidas.
- ✓ Ejecución del Servicio: Se ejecutan las actividades de identificación de vulnerabilidades a partir de programación de escaneos previamente definidos o a partir de requerimientos generados por necesidades institucionales, en atención a las especificaciones técnicas definidas. De igual manera, se ejecutan las actividades de administración y operación de la plataforma Tenable One.
- ✓ Seguimiento a la prestación del Servicio: Se verifica el avance en la ejecución de las actividades programadas o por demanda a partir del plan de escaneo periódico o a través del registro de casos por demanda. Se verifica a través del informe mensual la ejecución de las actividades asociadas a la ejecución de escaneos durante el periodo, en atención a las especificaciones técnicas definidas. Así mismo, se hace seguimiento a la ejecución de las actividades de administración y operación sobre la plataforma Tenable One.
- ✓ Finalización del Servicio: Se verifica el cumplimiento de los entregables y de la ejecución de las actividades de identificación y análisis de vulnerabilidades programadas o por demanda, en atención a las especificaciones técnicas; así

como las ejecutadas relacionadas con la administración y operación de la plataforma Tenable One.

Capacidades Disponibles del Servicio

- **Soluciones Tecnológicas**
  - ✓ Tenable One (Licenciadas por la Entidad)
- **Personal**
  - ✓ **Personal en Instalaciones del Proveedor**
    - ✓ Analista de Vulnerabilidades

Modelo de Prestación del Servicio:

En atención a la planeación y preparación del servicio se definen las actividades requeridas para la prestación del servicio, las cuales tienen tres enfoques de trabajo articulados, a saber: La identificación de vulnerabilidades sobre la infraestructura tecnológica; la identificación de vulnerabilidades sobre sitios y aplicaciones web; así como la ejecución de las actividades orientadas a la administración y operación de la plataforma Tenable One.

La ejecución del servicio debe garantizar que se desarrollen las actividades planeadas, orientadas a la identificación de vulnerabilidades en la infraestructura tecnológica y en los sitios y aplicaciones web institucionales, bien sea en atención a una programación definida o por demanda. De la misma manera, conforme a las especificaciones técnicas definidas y a la concertación entre las partes en la etapa de planeación para la prestación del servicio, se deberán ejecutar por parte del prestador del servicio las actividades de administración y operación de la plataforma Tenable One.

La entidad realizará actividades de seguimiento a partir de los informes de identificación y análisis de vulnerabilidades sobre activos informáticos de la infraestructura tecnológica, así como sobre los sitios y aplicaciones web; además del informe mensual sobre las actividades de identificación y análisis de vulnerabilidades ejecutadas y el informe mensual de las actividades de administración y operación de la plataforma Tenable One durante el periodo, buscando siempre el cumplimiento de las actividades encomendadas de acuerdo con las especificaciones técnicas definidas.

Entregables:

- ✓ Plan de Prestación del Servicio, que aborde las actividades configuración, mantenimiento de la plataforma, así como de identificación de vulnerabilidades sobre la infraestructura tecnológica y los sitios y aplicaciones web institucionales, en relación con la prestación de los servicios contratados.
- ✓ Informe de identificación y análisis de vulnerabilidades, incluyendo las recomendaciones para la remediación de los activos informáticos institucionales, a partir de los escaneos ejecutados sobre la infraestructura tecnológica institucional, bien sea programados o por demanda.
- ✓ Informe de identificación y análisis de vulnerabilidades, incluyendo las recomendaciones para la remediación de los activos informáticos institucionales, a partir de los escaneos ejecutados sobre los sitios y aplicaciones web institucionales, bien sea programados o por demanda.
- ✓ Informe mensual sobre las actividades ejecutadas en el periodo de identificación y análisis de vulnerabilidades sobre activos informáticos de la infraestructura tecnológica y sobre sitios y aplicaciones web.
- ✓ Informe mensual sobre la administración y operación de la plataforma Tenable One, detallando las actividades de mantenimiento, actualización, entre otras ejecutadas.

5. SERVICIO DE ETHICAL HACKING SOBRE RECURSOS INFORMÁTICOS INSTITUCIONALES

Objetivo:

Identificar potenciales vulnerabilidades de seguridad informática frente a ciberamenazas sobre los activos informáticos de la plataforma tecnológica institucional priorizados, a través de ejercicios de Ethical Hacking debidamente autorizados y controlados que permitan identificar planes de acción para actuar de manera oportuna en la mitigación de riesgos frente a ciberamenazas.

Características:

- ✓ Ejecutar las actividades de Ethical Hacking priorizadas por la entidad, a partir de “**solicitudes de ejecución de ejercicios de Ethical Hacking**” a demanda,

orientadas a identificar vulnerabilidades sobre los activos informáticos institucionales, siguiendo la metodología definida por la Entidad, utilizando las herramientas que el proveedor disponga para la ejecución de las actividades que permitan realizar actividades de reconocimiento, escaneo, enumeración, así como de intrusión, mantener el acceso y borrado de huellas a partir de los ejercicios priorizados.

Metodología:

- ✓ Planeación del Servicio: Se priorizan ejercicios de Ethical Hacking por demanda, que se abordaran a través de la metodología institucional definida, los cuales seran identificados y priorizados por la Entidad.
- ✓ Ejecución de Ejercicios de Ethical Hacking priorizados: Se ejecutarán las actividades basadas en ejercicios de Ethical Hacking priorizados, de acuerdo con el plan de trabajo definido. Las prácticas se ejecutarán de acuerdo con un plan de trabajo concertado, que incluya las responsabilidades y tiempos de las partes requeridas, en atención a las especificaciones técnicas definidas. Se respetará el plan de trabajo y su adecuación estará regida por la metodología propuesta por la Entidad de acuerdo con las especificaciones técnicas definidas.
- ✓ Seguimiento a la ejecución de Ejercicios de Ethical Hacking priorizados: Se realizarán actividades de seguimiento a la entrega de la documentación solicitada, a partir de la ejecución de las diferentes fases incluidas en la metodología, la cual será revisada y retroalimentada por la Entidad, para realizar los ajustes que puedan ser requeridos, de acuerdo con las especificaciones técnicas definidas.
- ✓ Finalización del Servicio: Se verifica el cumplimiento de los entregables y de la ejecución de las actividades asociadas a los planes de trabajo de los ejercicios de Ethical Hacking priorizados en el servicio, de acuerdo con las especificaciones técnicas definidas.

Metodología de Ethical Hacking Institucional

Planeación: La planeación será el escenario de concertación y preparación de las partes interesadas para definir los criterios, restricciones, límites y condiciones para la ejecución de las actividades de Ethical Hacking requeridas, que tiene como propósito poder mantener el control sobre las acciones, pero también minimizar que las mismas puedan afectar la disponibilidad parcial o total de los sistema de información y de los servicios de tecnologías de información y de las comunicaciones existentes, así como la prestación de los servicios misionales institucionales.

Fase 1 – Ethical Hacking: La Fase 1 del Ethical Hacking hace referencia al conjunto de acciones iniciales que se han venido identificando como parte general de cualquier actividad de Hacking Ethical convencional. En esta fase, el personal contratado podrá ejecutar acciones de reconocimiento, escaneo y enumeración. A partir de las actividades se generarán los informes pertinentes relacionados con la información identificada, tales como la superficie de ataque, la infraestructura de red y telecomunicaciones, la infraestructura de servidores, los puertos y protocolos disponibles, las vulnerabilidades, entre otras.

Revisión Fase 1: La socialización de la información producto de la ejecución de la fase 1 es realizada con la secretaría de innovación digital y de acuerdo con los resultados, la experticia del grupo que realiza la actividad y la necesidad de la Entidad, se determinan los activos informáticos críticos que se seleccionarán para continuar con las actividades de intrusión en la fase 2.
Fase 2 – Ethical Hacking: La Fase 2 del Ethical Hacking hace referencia al conjunto de acciones orientadas a la intrusión sobre los activos informáticos de la Entidad. En esta fase, el personal contratado podrá ejecutar acciones para obtener acceso a los activos informáticos, mantener el acceso, explotar vulnerabilidades, borrar huellas y generar el informe de intrusión correspondiente. A partir de las actividades se generarán los informes pertinentes relacionados con la información identificada, tales como las vulnerabilidades criticas explotadas, las cuentas de acceso comprometidas, las actividades de escalamiento de privilegios realizadas, las actividades de movimiento horizontal o vertical realizadas, así como las actividades para mantener el acceso y las realizadas para borrar las huellas del ataque. La Fase 2 se realiza teniendo en cuenta que los controles que actualmente tiene la entidad estarán operando de acuerdo con la configuración establecida a la fecha.

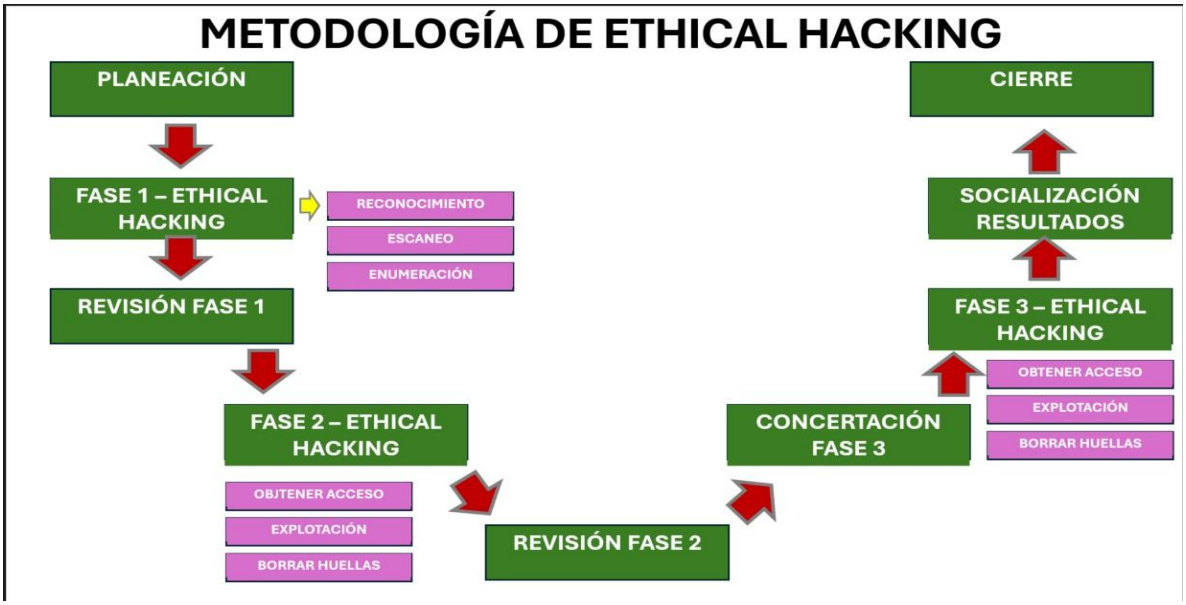
Revisión Fase 2: La socialización de la información producto de la ejecución de la fase 2 es realizada con la secretaría de innovación digital y de acuerdo con los resultados, la experticia del grupo que realiza la actividad y la necesidad de la Entidad, se determinan los activos informáticos críticos que se seleccionarán para continuar con las actividades de intrusión en la fase 3.

Concertación Fase 3: De acuerdo con el nivel de vulnerabilidades identificado, la criticidad de los activos, la necesidad de la Entidad, la experticia del grupo que realiza la actividad, se seleccionarán unos activos informáticos críticos, para volver a realizar la actividad de intrusión para la cual se podrán realizar de manera concertada las siguientes acciones: Unas variaciones en los controles de seguridad informática implementados, simulando el estado en el que los mismos no hubieran podido ser renovados o su disponibilidad dentro del servicio hubiera quedado anulada por algún tipo de problema administrativo, técnico o legal; lo cual incrementaría el nivel de riesgo de la Entidad; o repetir la actividad de intrusión a partir de ajustes realizados en la infraestructura, teniendo en cuenta los hallazgos de la fase 2; para verificar el estado de las remediaciones realizadas frente a las vulnerabilidades identificadas.

Fase 3 – Ethical Hacking: La Fase 3 del Ethical Hacking hace referencia al conjunto de acciones orientadas a la intrusión sobre los activos informáticos de la Entidad, con la diferencia de la fase 2, en que, por una parte, algunos controles fueran manipulados para incrementar el nivel de riegos de la Entidad, o porque se hubieran realizado remediaciones detectados en la fase 2 y fuera necesario corroborar la adecuada mitigación de riesgos con estas. En esta fase, el personal contratado podrá ejecutar acciones para obtener acceso a los activos informáticos, mantener el acceso, explotar vulnerabilidades, borrar huellas y generar el informe de intrusión correspondiente. A partir de las actividades se generarán los informes pertinentes relacionados con la información identificada, tales como las vulnerabilidades criticas explotadas, las cuentas de acceso comprometidas, las actividades de escalamiento de privilegios realizadas, las actividades de movimiento horizontal o vertical realizadas, así como las actividades para mantener el acceso y las realizadas para borrar las huellas del ataque.

Socialización de Resultados: La socialización de los resultados tiene como propósito colocar en contexto a la Secretaría de Innovación Digital sobre los riesgos materializados o el incremento en el nivel de riesgo por las situaciones identificadas en la ejecución de las actividades contratadas. Además, se proveen recomendaciones para fortalecer la seguridad informática de la organización frente a ciberamenazas.

Cierre: El cierre es la etapa que permite realizar la validación de toda la información recopilada a partir de las actividades realizadas, además facilita que se puedan dirimir las diferencias o realizar los ajustes o aclaraciones que puedan ser pertinentes para la validación final de los entregables acordados para la ejecución del proyecto.



Capacidades Disponibles del Servicio

- **Soluciones Tecnológicas**
  - ✓ (A cargo del proveedor incluidas como parte del servicio)
- **Personal**
  - ✓ **Personal en Instalaciones del Proveedor**
    - ✓ Especialistas en Ethical Hacking

Modelo de Prestación del Servicio:

En atención a la planeación y preparación del servicio se definen las actividades requeridas para la prestación del servicio, a partir de la priorización de ejercicios de ethical hacking por parte de la Entidad.

La ejecución del servicio debe garantizar que se ejecutan las actividades de Ethical Hacking priorizadas de acuerdo con la metodología institucional adoptada.

La entidad realizará actividades de seguimiento a partir de los informes sobre la ejecución de cada ejercicio de Ethical hacking priorizado.

Entregables:

- ✓ Informe sobre la ejecución a demanda de cada ejercicio de Ethical Hacking priorizado y autorizado, de acuerdo con la metodología institucional adoptada.

6. SERVICIO DE ADMINISTRACIÓN Y OPERACIÓN DE LA PLATAFORMA PARA LA PROTECCIÓN DE ACCESOS DE USUARIOS PRIVILEGIADOS

Objetivo:

Ejecutar las actividades de implementación, administración, mantenimiento y operación de la plataforma institucional para la protección de accesos con cuentas de usuario privilegiados, a través de personal certificado que permita controlar los accesos a los recursos informáticos institucionales priorizados de manera segura por parte de los usuarios responsables de cuentas privilegiadas, para fortalecer las capacidades de prevención, detección y respuesta ante eventos, alertas o incidentes de seguridad informática frente a ciberamenazas.

Características:

- ✓ Ejecutar las actividades requeridas orientada a la asociación de recursos informáticos (servidores, cuentas de usuario, configuración de accesos y protocolos de acceso, entre otros) priorizados para gestionar sus accesos privilegiados a través de la plataforma de gestión de accesos privilegiados institucional.
- ✓ Ejecutar las actividades de administración 5 x 8 de la plataforma de protección de accesos privilegiados a los recursos informáticos institucionales orientadas a garantizar el mantenimiento, la actualización y la disponibilidad de la prestación de los servicios de protección de accesos a las cuentas privilegiadas a las plataformas institucionales priorizadas.
- ✓ Ejecutar las actividades de operación 7 x 24 de la plataforma de protección de accesos privilegiados a los recursos informáticos institucionales orientada a garantizar la prestación de los servicios de control de accesos de los usuarios privilegiados a los recursos informáticos, la configuración de flujos de acceso de los usuarios, la autorización de requerimientos de acceso de usuarios privilegiados de acuerdo con los requerimientos definidos por la Entidad.
- ✓ Ejecutar las actividades requeridas para la atención de incidentes 7 x 24 sobre los componentes de la plataforma de protección de accesos privilegiados a los recursos informáticos institucionales.
- ✓ Ejecutar las actividades requeridas para desarrollar las condiciones, documentación y acciones para mantener actualizado un plan de contingencia para abordar situaciones de fallo o indisponibilidad de la plataforma para la protección de accesos privilegiados.
- ✓ Ejecutar las actividades de atención de requerimientos asociados a la administración (Mantenimiento, actualización, backup, configuración de reglas, administración de usuarios, atención de incidentes, entre otras) de la solución de protección de accesos privilegiados a los recursos informáticos institucionales.
- ✓ Ejecutar las actividades de atención de requerimientos asociados a la operación de la solución (flujos de aprobación de acceso de usuarios, recuperación de video de usuarios, cierre de sesión de usuarios conectados, configuración de parámetros del sistema, entre otros) de protección de accesos privilegiados a los recursos informáticos institucionales.

Metodología:

- ✓ Planeación del Servicio: Se definen las condiciones, formas y actividades a ejecutar durante la prestación del servicio, relacionadas con la asociación de recursos informáticos para la administración de accesos de cuentas privilegiadas, las acciones relacionadas con la administración de la plataforma,

el mantenimiento de la misma, y aquellas que se derivan de la operación, así como las relacionadas con la atención de requerimientos relacionados con la prestación de dicho servicio.

- ✓ Ejecución de la Prestación del Servicio: En atención a la planeación realizada, se ejecutan las actividades relacionadas con la asociación de Recursos Informáticos Priorizados que serán gestionados desde la plataforma de gestión de accesos privilegiados, de acuerdo con el plan de asociación de recursos informáticos y control de acceso, establecido por la Entidad. De igual manera, se ejecutan las actividades definidas en los planes de administración y de operación de la plataforma, de acuerdo con las especificaciones técnicas definidas. Así mismo, se ejecutan las actividades relacionadas con la atención de requerimientos de la administración y operación de la plataforma, así como la atención de incidentes que puedan afectar la disponibilidad de esta.
- ✓ Seguimiento a la prestación del Servicio: Se realiza seguimiento periódico a la prestación del servicio y a la ejecución de las diferentes actividades definidas. Se revisarán los informes de gestión sobre el cumplimiento de las actividades incluidas como parte del servicio, de acuerdo con las especificaciones técnicas definidas.
- ✓ Finalización del Servicio: Se verifica el cumplimiento de los entregables y de la ejecución de las actividades de administración y operación incluidas en el servicio, de acuerdo con las especificaciones técnicas definidas.

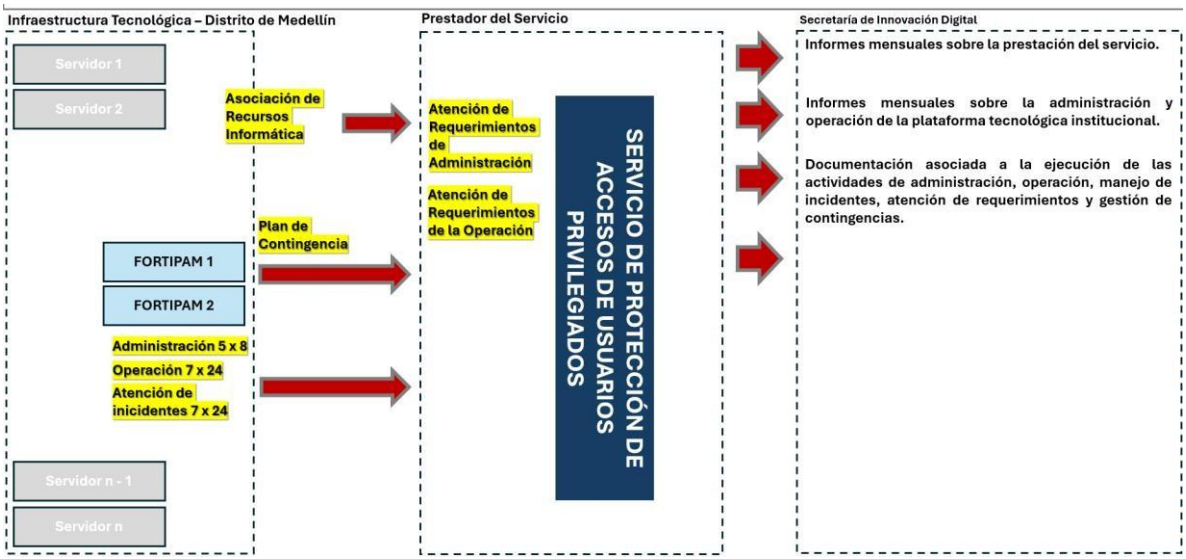
Capacidades Disponibles del Servicio

- ➢ **Soluciones Tecnológicas**
  - ✓ FortiPAM (Licenciamiento a cargo de la Entidad)
- ➢ **Personal**
  - ✓ **Personal en Instalaciones del Proveedor**
    - ✓ Especialista Nivel 2
    - ✓ Especialista Nivel 1

Modelo de Prestación del Servicio:

En atención a la planeación del servicio se definen las actividades requeridas para la prestación del servicio, teniendo en cuenta la asociación de los recursos informáticos a la plataforma, las actividades de administración, operación y atención de incidentes, así como la atención de requerimientos.

La ejecución del servicio debe garantizar que se ejecutan las actividades planificadas que permiten la operación de la plataforma de control de acceso de usuarios privilegiados. Adicionalmente se ejecutan las actividades de administración, operación y atención de incidentes previstas, así como la atención de requerimientos relacionados con la administración y operación de la plataforma.



La entidad realizará actividades de seguimiento a partir de los informes mensuales para la asociación de recursos informáticos, los informes mensuales sobre la administración y operación de la plataforma adquirida.

Entregables:

- ✓ Plan de prestación del servicio, orientado a identificar las actividades asociadas a la administración, operación, mantenimiento, atención de requerimientos asociados al control de acceso de usuarios privilegias, así como sobre la gestión de incidentes sobre la plataforma que soporta la prestación de dicho servicio.
- ✓ Informe mensual sobre la prestación del servicio, que incluyen actividades relacionadas con el avance en la asociación de recursos informáticos (servidores, cuentas de usuario, configuración de accesos y protocolos de acceso, entre otros) priorizados, así como con la atención de requerimientos de administración y de operación relacionados con la prestación del servicio.
- ✓ Informe mensual sobre la administración y operación de la plataforma tecnológica institucional que soporta la gestión de accesos privilegiados.
- ✓ Documentación asociada a la ejecución de las actividades de administración, operación, manejo de incidentes, atención de requerimientos y gestión de contingencias.

7. SERVICIO DE ANÁLISIS FORENSE DIGITAL EN EQUIPOS DE COMPUTO

Objetivo:

Ejecutar las actividades Inicio de cadena de custodia, adquisición de imagen forense, Extracción y recuperación de evidencia sobre las imágenes forenses, así como de Clasificación de contenido relevante y hallazgos a través de técnicas especializadas de análisis forense que permitan contar con información para tomar

decisiones relacionadas con el tratamiento de información almacenada en diez (10) equipos de cómputo institucionales.

Características:

- ✓ Ejecutar las actividades de inicio de cadena de custodia y adquisición de imagen forense, a través de técnicas especializadas de análisis forense, a partir de una "solicitud a demanda de análisis forense de equipo de cómputo institucional específico".
- ✓ Ejecutar las actividades de extracción y recuperación de evidencia sobre las imágenes forenses, a través de técnicas especializadas de análisis forense, a partir de una "solicitud a demanda de análisis forense de equipo de cómputo institucional específico".
- ✓ Ejecutar las actividades de clasificación de contenido relevante y hallazgos, a través de técnicas especializadas de análisis forense, a partir de una "solicitud a demanda de análisis forense de equipo de cómputo institucional específico".

Metodología:

- ✓ Planeación del Servicio: Se definen las condiciones para solicitar y atender el servicio, en atención a las necesidades de la Entidad y la metodología de ejecución de las actividades propuesta por el prestador del servicio. Las necesidades identificadas se caracterizarán a través de "solicitudes de análisis forense de equipos de cómputo institucionales específicos", en el que se determinan las características de identificación y ubicación del equipo de cómputo sobre el que se aplicará el servicio, de acuerdo con las especificaciones técnicas definidas.
- ✓ Ejecución de las actividades de Análisis Forense: Se ejecutan las actividades definidas por el prestador del servicio de acuerdo con la metodología concertada y con las especificaciones técnicas del servicio.
- ✓ Seguimiento a la prestación del Servicio: Se realiza seguimiento a la prestación del servicio y a la ejecución de las diferentes etapas definidas. Se realizan informes sobre la ejecución de las actividades por cada solicitud de análisis forense de equipos de cómputo institucional específico, de acuerdo con las especificaciones técnicas definidas.
- ✓ Finalización del Servicio: Se verifica el cumplimiento de la ejecución de las actividades de análisis forense de equipo de cómputo institucionales específicos priorizados, de acuerdo con las especificaciones técnicas definidas.

Capacidades Disponibles del Servicio

- ➢ **Soluciones Tecnológicas**
  - ✓ Herramientas a cargo del proveedor)
- ➢ **Personal**

- ✓ **Personal en Instalaciones del Proveedor**
- ✓ Especialista en Análisis Forense

Modelo de Prestación del Servicio:

En atención a la planeación del servicio se definen las actividades requeridas para la atención de solicitudes de análisis forense de equipos de cómputo institucionales por parte del prestador de servicio.

La ejecución del servicio debe garantizar que, a partir de una solicitud de análisis forense de equipos de cómputo institucionales, se ejecutan las actividades previstas de acuerdo con la metodología del proveedor para la prestación del servicio solicitado.

La entidad realizará actividades de seguimiento a partir de los informes realizados por el proveedor en relación con las actividades forenses aplicados sobre los equipos de cómputo institucionales.

Entregables:

✓ Informe sobre las actividades forenses aplicadas sobre cada equipo de cómputo institucional específico, a partir de la solicitud a demanda realizada.

8. SERVICIO DE EVALUACIÓN INTEGRAL DE LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN DE GESTIÓN DOCUMENTAL INSTITUCIONAL

Objetivo:

Ejecutar las actividades de evaluación del estado de la seguridad del sistema de gestión documental, a través de una metodología que permita la evaluación diagnostica, la evaluación de vulnerabilidades, la ejecución de actividades de ethical hacking, de evaluación del cumplimiento, la evaluación de la Seguridad del segmento de red donde se aloja el sistema de información, la evaluación de la seguridad física, la evaluación de la Seguridad de proveedores, así como la evaluación de la Seguridad Interna, para identificar potenciales vulnerabilidades que permitan identificar y priorizar planes de remediación específicos.

Características:

- ✓ Ejecutar las actividades de evaluación diagnostica, a partir de una “solicitud a demanda de evaluación diagnostica” emitida por la Entidad.
- ✓ Ejecutar las actividades de evaluación de vulnerabilidades a partir de una “solicitud a demanda de evaluación de vulnerabilidades”, emitida por la Entidad.

- ✓ Ejecutar actividades de ethical hacking a partir de una “solicitud a demanda de ejecución de ejercicios de ethical hacking”, emitida por la Entidad.
- ✓ Ejecutar actividades de evaluación del cumplimiento de los controles priorizados de acuerdo con lo dispuesto en el anexo A de la NTC ISO 27001, a partir de una “solicitud a demanda de ejecución de evaluación del cumplimiento”, emitida por la Entidad.
- ✓ Ejecutar las actividades de evaluación del segmento de red de datos priorizado, a partir de una “solicitud a demanda de ejecución de evaluación de segmentos de red institucionales”, emitida por la Entidad.
- ✓ Ejecutar las actividades de evaluación de la seguridad física priorizada, a partir de una “solicitud a demanda de ejecución de evaluación de la seguridad física”, emitida por la Entidad.
- ✓ Ejecutar las actividades de evaluación de la seguridad de los proveedores priorizados, a partir de una “solicitud a demanda de ejecución de evaluación de la seguridad de proveedores”, emitida por la Entidad.
- ✓ Ejecutar las actividades de evaluación de la seguridad interna priorizada, a partir de una “solicitud a demanda de ejecución de evaluación de la seguridad interna”, emitida por la Entidad.

Metodología:

- ✓ Planeación del Servicio: Se definen las condiciones para ejecutar a demanda las actividades de evaluación integral priorizadas, que permitan generar las condiciones de verificación de la seguridad asociadas al sistema de información de gestión documental, de acuerdo con las especificaciones técnicas definidas.
- ✓ Ejecución de las actividades de evaluación de la seguridad: Se ejecutan a demanda las actividades priorizadas, a partir de las solicitudes especificas definidas por la Entidad.
- ✓ Seguimiento a la prestación del Servicio: Se realiza seguimiento a la prestación del servicio y a la ejecución a demanda de las diferentes actividades priorizadas.
- ✓ Finalización del Servicio: Se verifica el cumplimiento de los informes asociados a las actividades priorizadas y ejecutadas por el prestador del servicio a demanda.

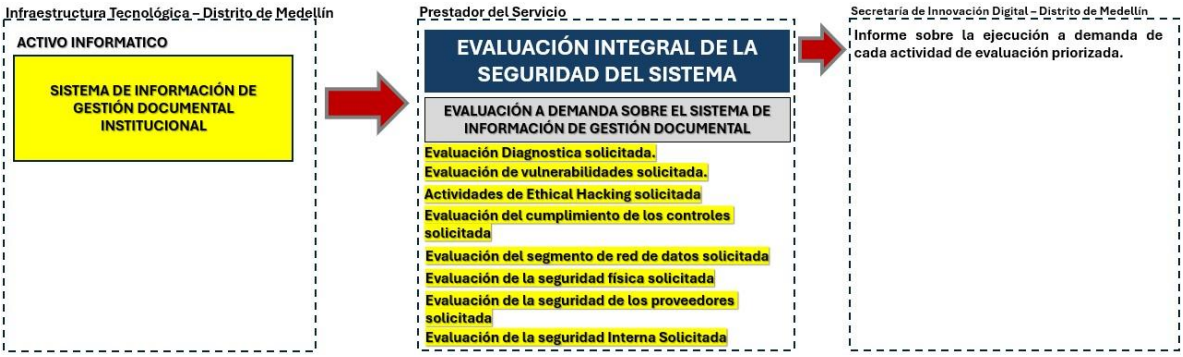
Capacidades Disponibles del Servicio

- ➢ **Soluciones Tecnológicas**
- ✓ (A cargo del proveedor)
- ➢ **Personal**
  - ✓ **Personal en Instalaciones del Proveedor**
    - ✓ (A cargo del proveedor)

Modelo de Prestación del Servicio:

En atención a la planeación del servicio se definen las actividades priorizadas para la evaluación de la seguridad del sistema de información mercurio y la infraestructura tecnológica subyacente.

La ejecución del servicio debe garantizar que se ejecutan las actividades priorizadas, de acuerdo con la metodología del proveedor para la prestación del servicio solicitado.



La entidad realizará actividades de seguimiento verificando los informes realizados a partir de las actividades ejecutadas en atención a las actividades de evaluación solicitadas.

Entregables:

- ✓ Informe sobre la ejecución a demanda de cada actividad de evaluación priorizada.

IMAGEN CORPORATIVA:

Durante la ejecución de la Orden de Servicio será utilizada solo la imagen de la ESU por lo tanto, todos los documentos que sean producidos por el Aliado en razón de la ejecución de esta Orden de Servicio deberán ser aprobadas por la ESU.

VALOR DE LA ORDEN DE SERVICIO: El valor de la presente orden de servicios es de **SETECIENTOS CINCUENTA Y SIETE MILLONES DOSCIENTOS OCHENTA Y OCHO MIL SEISCIENTOS NOVENTA Y SIETE PESOS M/L ($757.288.697)** impuestos incluidos.

Servicios Recurrentes	$ 114.333.631
Servicios a Demanda	$ 642.955.066
TOTAL	**$ 757.288.697**

La ESU pagará al Contratista los servicios que efectivamente hayan sido prestados, cuyos valores hayan sido aprobados por la Supervisión, por lo que procederá una vez vencido el plazo, a liberar los valores que no hayan sido ejecutados.

INFORMACIÓN PRESUPUESTAL ORDEN DE SERVICIO:

Contrato Interadministrativo:	4600105618 de 2025
Certificado de Disponibilidad Presupuestal:	2025001145
Certificado de Registro Presupuestal:	2025001296
Centro de costos:	21368
Rubro al presupuesto:	23502080000012-1/23502080000013-1
Descripción al Rubro:	GESTION Y PROTECCION INFORMATICA -SERVICIOS RECURRENTES/GESTION Y PROTECCION INFORMATICA - SERVICIOS A DEMANDA
Requerimiento N°:	**20250007952**

Para efectos de consecutivo en la parte presupuestal, esta orden hace las veces de la No. 1

FORMA DE PAGO: La ESU cancelará el valor de la orden de servicio mediante pagos parciales; previa/o aprobación de las garantías expedida por la Unidad de Gestión Jurídica y recibo de cumplimiento de la prestación del servicio por parte del supervisor del Contrato del cual se deriva la Orden de Servicio. Acorde a los siguientes parámetros:

- La respectiva factura debe cumplir con los requisitos de las normas fiscales establecidas en el artículo 617 del Estatuto Tributario. La fecha de la factura debe corresponder al mes de su elaboración, y en ella constará el número del contrato y, el concepto del bien o servicio que se está cobrando.
- El proveedor deberá acreditar la efectiva prestación del servicio por medio de una constancia de recibo firmada por el beneficiario. Una vez aprobada la constancia de recibo por parte del supervisor del contrato, éste emitirá el recibo a entera satisfacción del servicio contratado.
- Las retenciones en la fuente a que hubiere lugar y todo impuesto, tasa o contribución directa o indirecta, Nacional, Departamental o Municipal que se cause por razón de la celebración, ejecución y pago de este Contrato serán a cargo exclusivo del Aliado.
  Nota: Si la propuesta presentada supera los 6.000 UVT, el contrato resultante será gravado con el impuesto de timbre de conformidad con lo establecido en el Estatuto Tributario, las normas que lo modifican o complementan y el contrato
- Una vez recibida a satisfacción la factura o cuenta de cobro correspondiente, la ESU tendrá treinta (30) días calendario para proceder a su pago. En caso de incurrir en mora en los pagos, la ESU reconocerá al Contratista un interés equivalente al DTF anual de manera proporcional al tiempo de retraso.

- Al momento de entregar la factura, ésta deberá estar acompañada con el certificado de pago de aporte de sus empleados al Sistema de Seguridad Social Integral y a las entidades que administran recursos de naturaleza parafiscal; y la carta donde se especifique la entidad y el número de cuenta bancaria a la cual se le deberá realizar el pago.

PLAZO DE LA ORDEN DE SERVICIO: Hasta el TREINTA Y UNO (31) de diciembre de 2025 contados a partir de la aprobación de la garantía única de cumplimiento por la Unidad de Gestión Jurídica.

PLAZO PARA LA SUSCRIPCIÓN DE LA PRESENTE ORDEN DE SERVICIO: Al recibo del presente documento, el CONTRATISTA, contará con máximo de dos (2) días hábiles para la suscripción y legalización del mismo, y si es del caso para allegar las pólizas modificadas, so pena de que se declare el incumplimiento y que se puedan hacer efectiva las garantías constituidas a favor del CONTRATANTE.

SUPERVISIÓN: El seguimiento técnico, administrativo, financiero, contable y jurídico del cumplimiento a satisfacción del presente objeto contractual se realizará por Profesional universitario, o quien sea designado por la Subgerente de servicios. En todo caso la designación podrá hacerse directamente por la Gerencia.

GARANTÍAS: El Contratista se obliga a constituir a favor de “La Empresa para la Seguridad y Soluciones Urbanas - ESU Y Secretaría de Innovación del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín”, una garantía única de las expedidas para Entidades estatales que ampare el cumplimiento de las obligaciones contractuales, otorgada por una compañía de seguros autorizada para operar en Colombia por la Superintendencia Financiera y preferiblemente con poderes decisorios en la Ciudad de Medellín:

Garantías y Mecanismos de cobertura del riesgo: El Contratista se obliga a garantizar el cumplimiento de las obligaciones surgidas a favor de la ESU, con ocasión de la ejecución del contrato, de acuerdo con lo siguiente:

- ✓ **Cumplimiento:** Por el veinte por ciento (20%) del valor del mismo, con una vigencia igual a la duración del contrato y seis (6) meses más.
- ✓ **Calidad del servicio:** Por el diez por ciento (10%) del valor del mismo, con una vigencia igual a la duración del contrato y seis (6) meses más.
- ✓ **Salarios, prestaciones sociales e indemnizaciones al personal: hasta** Por el diez por ciento (10%) del valor del mismo, con una vigencia igual a la duración del contrato y tres (3) años más.
- ✓ **Responsabilidad civil extracontractual:** Doscientos (200) SMMLV con una vigencia igual al plazo del contrato.

PARÁGRAFO 1: El contratista deberá modificar el monto de la garantía cada vez que sea necesario, en razón del incremento del contrato, la afectación por

reclamaciones o por el cambio de vigencia y actualización de aquellos valores que estén tasados en SMMLV. Si el contratista se negare a constituir o a reponer la garantía exigida, la ESU directamente solicitará a la Compañía de Seguros la modificación de la misma, además podrá dar por terminado el contrato en el estado en que se encuentre, sin que haya lugar a reconocer o pagar indemnización alguna.

PARÁGRAFO 2: Al recibo del contrato, el contratista contará con máximo dos (2) días hábiles para la constitución de la póliza única de cumplimiento y entrega de la documentación respectiva.

DOCUMENTOS INTEGRALES: Hacen parte de la presente orden de servicio el Contrato Marco 202500142_1 y demás documentos emanados con ocasión de esta. Las estipulaciones pactadas mediante el presente documento no constituyen novación al contrato marco del cual se derivan, el cual encuentra vigente.

ACEPTACIÓN ORDEN DE SERVICIO: En aceptación de lo anterior, la fecha de suscripción es el día quince (15) de diciembre de 2025.

POR LA ESU,

ANGELICA LÓPEZ GARCES
Subgerente de Servicios

POR EL CONTRATISTA,

MÓNICA MARÍA GIRALDO GÓMEZ
Representante Legal

Aprobó	Kamal abdul nassar	Secretario General	
Aprobó	Nathalia Restrepo Caro	Subgerente Administrativa y Financiera	
Revisó	Cristian Ferney López Castrillón	Profesional Especializado - Unidad de Gestión Jurídica	
Proyectó	Tatiana Silva Pulido	Profesional Universitario - Unidad de Compras y Contratación	

Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes, por tanto, bajo nuestra responsabilidad lo presentamos para firma.